Documentação do ONTAP 9

ONTAP 9

NetApp
December 20, 2024

Índice

Documentação do ONTAP 9

Notas de lançamento

Destaques do lançamento do ONTAP 9

Cada versão do software de gerenciamento de dados ONTAP 9 oferece recursos novos e aprimorados que melhoram os recursos, a capacidade de gerenciamento, o desempenho e as ofertas de segurança do ONTAP.

Além desses destaques, você pode encontrar uma cobertura abrangente por versão de todos os recursos novos e aprimorados introduzidos nas versões recentes do ONTAP.

- Saiba mais "Novos e aprimorados recursos do ONTAP MetroCluster"sobre .
- Saiba mais "Suporte novo e aprimorado para plataformas FAS, ASA e AFF e switches compatíveis"sobre .
- Saiba mais sobre as atualizações do "API REST do ONTAP".

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Para atualizar para a versão mais recente do ONTAP, Atualize para a versão mais recente do ONTAPconsulte e. Quando devo atualizar o ONTAP?

Destaques do ONTAP 9.16,1

O ONTAP 9.16,1 oferece recursos novos e aprimorados nas áreas de gerenciamento de segurança, proteção de dados, rede, gerenciamento de SAN e gerenciamento de storage. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.16,1consulte .

- Melhorias na verificação multi-admin (MAV)

  O ONTAP 9.16,1 adiciona mais comandos à estrutura MAV para proteção adicional contra insiders maliciosos. Esses aprimoramentos incluem gerenciamento de muitos grupos de consistência (CG), Vscan e Autonomous ransomware Protection (ARP) e comandos de configuração NVMe.

- Proteção autônoma contra ransomware com aprimoramentos de AI (ARP/AI)

  O ARP foi atualizado com novos recursos de AI, permitindo que a TI detete e responda a ataques de ransomware com 99% de precisão e recall. Como a IA é treinada em um conjunto de dados abrangente, não há mais um período de aprendizado para o ARP sendo executado em volumes FlexVol e o ARP/AI começa no modo ativo imediatamente. O ARP/AI também apresenta um recurso de atualização automática independente de uma atualização do ONTAP para garantir proteção e resiliência constantes contra as ameaças mais recentes.

- NVMe/TCP em TLS 1,3

  Proteja o NVMe/TCP "por cabo" na camada de protocolo com uma configuração simplificada e melhor desempenho em comparação com o IPSec.

- Suporte para descarga de hardware IPsec para novas placas de rede

  O ONTAP 9.16,1 oferece maior desempenho de criptografia "over-the-wire" ao utilizar a funcionalidade de descarga de hardware IPSec em placas de descarga introduzida para todas as novas plataformas de

sistemas AFF A-series e AFF-C.

- Suporte para alocação de espaço NVMe

  A realocação de espaço (também chamada de "perfuração" e "desmapear") agora é compatível com namespaces NVMe. O dellocation de espaço ajuda volumes com thin Provisioning e namespaces NVMe a recuperar espaço não usado quando os dados são excluídos pelo aplicativo host. Isso melhora muito a eficiência geral de armazenamento, especialmente com sistemas de arquivos que têm alta rotatividade de dados.

- Balanceamento de capacidade avançado para volumes FlexGroup

  O NetApp FlexGroup volumes pode, opcionalmente, distribuir dados de arquivos em vários volumes constituintes de back-end, reduzindo gargalos de desempenho e adicionando consistência na capacidade de balanceamento nos volumes constituintes do back-end.

Destaques do ONTAP 9.15,1

O ONTAP 9.15,1 oferece recursos novos e aprimorados nas áreas de gerenciamento de segurança, proteção de dados e suporte a workloads nas. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.15,1consulte .

- "Suporte para novos sistemas AFF A-series, storage criado para AI"

  O ONTAP 9.15,1 dá suporte aos novos sistemas AFF A1K, AFF A90 e AFF A70 de alta performance, desenvolvidos para a próxima geração de workloads de negócios, como treinamento e inferência de AI/ML. Essa nova classe de sistemas fornece até o dobro da performance das ofertas existentes do AFF A-series e fornece eficiência de storage aprimorada "sempre ativa", sem interrupções de performance.

- Aplicativos de backup do Windows e links simbólicos em estilo Unix

  Começando com ONTAP 9.15,1, você também tem a opção de fazer backup do próprio link simbólico em vez dos dados para os quais ele aponta. Isso pode fornecer vários benefícios, incluindo melhor desempenho de seus aplicativos de backup. Você pode ativar o recurso usando a CLI do ONTAP ou a API REST.

- Autorização dinâmica

  O ONTAP 9.15,1 introduz uma estrutura inicial para autorização dinâmica, um recurso de segurança que pode determinar se um comando emitido por uma conta de administrador deve ser negado, solicitado para autenticação adicional ou autorizado a prosseguir. As determinações são baseadas na pontuação de confiança da conta do usuário, levando em conta fatores como hora do dia, localização, endereço IP, uso confiável do dispositivo e histórico de autenticação e autorização do usuário.

- Escopo expandido de impactos para verificação de vários administradores

  O ONTAP 9.15,1 RC1 adiciona mais de uma centena de novos comandos à estrutura MAV para proteção adicional contra insiders maliciosos.

- NFS em TLS

  Proteja os dados "por cabo" na camada de protocolo com configuração simplificada em comparação com outras tecnologias, como IPSec e NFS Kerberos. Este recurso está incluído como visualização pública no momento. Para obter mais informações sobre essa capacidade, entre em Contato com sua equipe de vendas para obter informações adicionais.

- Suporte de criptografia TLS 1,3 para peering de cluster e muito mais

  O ONTAP 9.15,1 apresenta suporte de criptografia TLS 1,3 para criptografia de peering de cluster, FlexCache, SnapMirror e armazenamento S3. Aplicativos como o FabricPool, o armazenamento de Blobs de páginas do Microsoft Azure e a nuvem do SnapMirror continuam a usar o TLS 1,2 para a versão 9.15.1.

- Suporte para tráfego SMTP através de TLS

  Transfira dados do AutoSupport com segurança por e-mail com suporte a TLS.

- Sincronização ativa do SnapMirror para configurações ativo-ativo simétricas

  Essa nova funcionalidade fornece replicação bidirecional síncrona para continuidade dos negócios e recuperação de desastres. Proteja o acesso a dados para workloads SAN críticos com acesso de leitura e gravação simultâneos aos dados em vários domínios de falha, permitindo operações ininterruptas e minimizando o tempo de inatividade durante desastres ou falhas do sistema.

- FlexCache writeback

  O FlexCache writeback permite que os clientes gravem localmente em volumes FlexCache, reduzindo a latência e melhorando o desempenho em comparação à gravação diretamente no volume de origem. Os dados recém-gravados são replicados assincronamente de volta ao volume de origem.

- NFSv3 sobre RDMA

  O suporte NFSv3 sobre RDMA pode ajudá-lo a atender aos requisitos de alto desempenho, fornecendo acesso de baixa latência e alta largura de banda via TCP.

Destaques do ONTAP 9.14,1

O ONTAP 9.14,1 oferece recursos novos e aprimorados nas áreas de FabricPool, proteção anti-ransomware, OAuth e muito mais. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.14,1consulte .

- Redução de reservas no WAFL

  O ONTAP 9.14,1 introduz um aumento imediato de cinco por cento no espaço utilizável em sistemas FAS e Cloud Volumes ONTAP, reduzindo a reserva WAFL em agregados com 30 TB ou mais.

- Melhorias no FabricPool

  O FabricPool aumenta leia o desempenhoe permite a gravação direta na nuvem, reduzindo o risco de ficar sem espaço e reduzindo os custos de storage movendo dados inativos para uma camada de storage mais barata.

- "Suporte para OAuth 2,0"

  O ONTAP suporta a estrutura OAuth 2,0, que pode ser configurada usando o Gerenciador de sistema. Com o OAuth 2,0, você pode fornecer acesso seguro ao ONTAP para estruturas de automação sem criar ou expor IDs de usuário e senhas a scripts de texto simples e runbooks.

- "Aprimoramentos de proteção autônoma contra ransomware (ARP)"

  O ARP concede mais controle sobre a segurança de eventos, permitindo que você ajuste as condições que criam alertas e reduzindo a possibilidade de falsos positivos.

- Ensaio de recuperação de desastres do SnapMirror no Gerente de sistemas

  O System Manager fornece um fluxo de trabalho simples para testar facilmente a recuperação de desastres em um local remoto e limpar após o teste. Esse recurso permite testes mais fáceis e frequentes e maior confiança nos objetivos de tempo de recuperação.

- S3 suporte de bloqueio de objetos

  O ONTAP S3 oferece suporte ao comando API de bloqueio de objeto, permitindo que você proteja os dados gravados no ONTAP com S3 contra exclusão usando comandos padrão da API S3 e garanta que os dados importantes sejam protegidos pelo período de tempo apropriado.

- Cluster e volume marcação

  Adicione tags de metadados a volumes e clusters, que seguem os dados conforme eles são migrados do local para a nuvem e revertidos.

Destaques do ONTAP 9.13,1

O ONTAP 9.13,1 oferece recursos novos e aprimorados nas áreas de proteção contra ransomware, grupos de consistência, qualidade do serviço, gerenciamento de capacidade do locatário e muito mais. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.13,1consulte .

- Aprimoramentos de proteção autônoma contra ransomware (ARP):
  - Capacitação automática

    Com o ONTAP 9.13,1, o ARP passa automaticamente do treinamento para o modo de produção após ter dados de aprendizado suficientes, eliminando a necessidade de um administrador habilitá-lo após o período de 30 dias.

  - Suporte à verificação de vários administradores

    Os comandos de desativação ARP são suportados pela verificação multi-admin, garantindo que nenhum administrador pode desativar o ARP para expor os dados a potenciais ataques de ransomware.

  - Suporte à FlexGroup

    O ARP suporta FlexGroups começando com ONTAP 9.13,1. O ARP pode monitorar e proteger FlexGroups que abrangem vários volumes e nós no cluster, permitindo que até mesmo os maiores conjuntos de dados sejam protegidos com ARP.

- Monitoramento de desempenho e capacidade para grupos de consistência no System Manager

  O monitoramento de desempenho e capacidade fornece detalhes para cada grupo de consistência, permitindo que você identifique e relate rapidamente problemas potenciais no nível da aplicação, em vez de apenas no nível do objeto de dados.

- Gerenciamento de capacidade do locatário

  Os clientes e fornecedores de serviços que alocação a vários clientes podem definir um limite de capacidade em cada SVM, permitindo que os locatários realizem provisionamento de autoatendimento sem o risco de uma capacidade excessivamente demorada no cluster.

- Qualidade de Serviço tetos e pisos

  O ONTAP 9.13,1 permite agrupar objetos como volumes, LUNs ou arquivos em grupos e atribuir um limite de QoS (IOPs máximos) ou andar (IOPs mínimos), melhorando as expectativas de desempenho do aplicativo.

Destaques do ONTAP 9.12,1

O ONTAP 9.12,1 oferece recursos novos e aprimorados nas áreas de fortalecimento da segurança, retenção, desempenho e muito mais. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.12,1consulte .

- Instantâneos invioláveis

  Com a tecnologia SnapLock, as cópias Snapshot podem ser protegidas contra exclusões na origem ou no destino.

  Retenha mais pontos de recuperação protegendo snapshots no storage primário e secundário contra a exclusão por invasores de ransomware ou administradores desonestos.

- Aprimoramentos de proteção autônoma contra ransomware (ARP)

  Habilite imediatamente a proteção inteligente e autônoma contra ransomware em storage secundário, com base no modelo de triagem já concluído para o storage primário.

  Após um failover, identifique instantaneamente potenciais ataques de ransomware no storage secundário. Um Snapshot é imediatamente retirado dos dados que estão começando a ser afetados e os administradores são notificados, o que ajuda a parar um ataque e aprimorar a recuperação.

- FPolicy

  Ativação com um clique do FPolicy do ONTAP para permitir o bloqueio automático de arquivos mal-intencionados conhecidos a ativação simplificada ajuda a proteger contra ataques típicos de ransomware que usam extensões de arquivo conhecidas e comuns.

- Fortalecimento da segurança: Registro de retenção inviolável

  O login de retenção à prova de violações no ONTAP seguro que as contas de administrador comprometidas não podem ocultar ações maliciosas. O Admin e o histórico do usuário não podem ser alterados ou excluídos sem o conhecimento do sistema.

  Registre e audite todas as ações de administração, independentemente da origem, garantindo que todas as ações que impactam os dados sejam capturadas. Um alerta é gerado sempre que os logs de auditoria do sistema foram adulterados de qualquer forma notificando os administradores da alteração.

- Fortalecimento da segurança: Autenticação multifator expandida

  A autenticação multifator (MFA) para CLI (SSH) suporta dispositivos token de hardware físico Yubikey, garantindo que um invasor não possa acessar o sistema ONTAP usando credenciais roubadas ou um sistema cliente comprometido. O Cisco DUO é compatível com MFA no Gerenciador de sistemas.

- Dualidade ficheiro-objeto (acesso multiprotocolo)

  A dualidade ficheiro-objeto permite o acesso nativo de leitura e gravação do protocolo S3 à mesma fonte de dados que já tem acesso ao protocolo nas. Você pode acessar ao mesmo tempo o storage como

arquivos ou como objetos da mesma fonte de dados, eliminando a necessidade de cópias duplicadas de dados para uso com diferentes protocolos (S3 ou nas), como análises que usam dados de objeto.

- Rebalanceamento do FlexGroup

  Se os componentes do FlexGroup ficarem desequilibrados, o FlexGroup poderá ser rebalanceado e gerenciado sem interrupções com a CLI, a API REST e o Gerenciador de sistemas. Para um desempenho ideal, os membros constituintes dentro de um FlexGroup devem ter sua capacidade usada distribuída uniformemente.

- Melhorias na capacidade de storage

  A reserva de espaço da WAFL foi significativamente reduzida, fornecendo até 400 TIB mais capacidade utilizável por agregado.

Destaques do ONTAP 9.11,1

O ONTAP 9.11,1 oferece recursos novos e aprimorados nas áreas de segurança, retenção, desempenho e muito mais. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.11,1consulte .

- Verificação multi-admin

  A verificação multi-admin (MAV) é uma abordagem nativa da indústria para verificação, que exige várias aprovações para tarefas administrativas confidenciais, como a exclusão de um Snapshot ou volume. As aprovações necessárias em uma implementação MAV evitam ataques maliciosos e alterações acidentais nos dados.

- Melhorias na proteção Autonomous ransomware

  O Autonomous ransomware Protection (ARP) usa o aprendizado de máquina para detetar ameaças de ransomware com maior granularidade, permitindo que você identifique ameaças rapidamente e acelere a recuperação em caso de violação.

- SnapLock Compliance para FlexGroup volumes

  Proteja os dados com bloqueio de arquivos WORM para workloads, que não podem ser alterados ou excluídos.

- Eliminação assíncrona do diretório

  Com o ONTAP 9.11,1, a exclusão de arquivos ocorre em segundo plano do sistema ONTAP, permitindo que você exclua facilmente grandes diretórios e, ao mesmo tempo, elimine impactos no desempenho e na latência na e/S do host

- S3 melhorias

  Simplifique e expanda os recursos de gerenciamento de dados de objeto do S3 com o ONTAP com endpoints de API adicionais e controle de versão de objetos no nível do bucket, permitindo que várias versões de um objeto sejam armazenadas no mesmo bucket.

- Melhorias no System Manager

  O System Manager oferece suporte a recursos avançados para otimizar recursos de storage e melhorar o gerenciamento de auditoria. Essas atualizações incluem habilidades aprimoradas de gerenciamento e

configuração de agregados de storage, visibilidade aprimorada da análise do sistema e visualização de hardware para sistemas FAS.

Destaques do ONTAP 9.10,1

O ONTAP 9.10,1 oferece recursos novos e aprimorados nas áreas de proteção de segurança, análise de performance, suporte ao protocolo NVMe e opções de backup de storage de objetos. Para obter uma lista completa de novos recursos e aprimoramentos, O que há de novo no ONTAP 9.10,1consulte .

- Proteção autônoma contra ransomware

  O Autonomous ransomware Protection cria automaticamente uma cópia Snapshot do seu volume e alerta os administradores quando uma atividade anormal é detetada, permitindo que você detete rapidamente ataques de ransomware e se recupere com mais rapidez.

- Melhorias no System Manager

  O System Manager faz o download automático de atualizações de firmware para discos, gavetas e processadores de serviço, além de fornecer novas integrações com o Active IQ Digital Advisor (também conhecido como consultor digital), o BlueXP e o gerenciamento de certificados. Essas melhorias simplificam a administração e mantêm a continuidade dos negócios.

- Melhorias na análise do sistema de arquivos

  O File System Analytics fornece telemetria adicional para identificar os principais arquivos, diretórios e usuários em seu compartilhamento de arquivos, permitindo identificar problemas de performance de workload para melhorar o Planejamento e a implementação de QoS.

- Compatibilidade com NVMe em TCP (NVMe/TCP) para sistemas AFF

  Obter alta performance e reduzir o TCO da SAN empresarial e workloads modernos no sistema AFF quando você usa NVMe/TCP em sua rede Ethernet existente.

- Compatibilidade com NVMe em Fibre Channel (NVMe/FC) para sistemas NetApp FAS

  Usar o protocolo NVMe/FC nos arrays híbridos para permitir a migração uniforme para o NVMe.

- Backup de nuvem híbrida nativa para storage de objetos

  Proteja seus dados do ONTAP S3 com seus destinos de storage de objetos à sua escolha. Use a replicação do SnapMirror para fazer backup no storage local com o StorageGRID, na nuvem com Amazon S3 ou em outro bucket do ONTAP S3 nos sistemas NetApp AFF e FAS.

- Bloqueio global de arquivos com o FlexCache

  Garanta a consistência do arquivo nos locais de cache durante as atualizações para arquivos de origem na origem com bloqueio global de arquivos usando o FlexCache. Esse aprimoramento permite bloqueios exclusivos de leitura de arquivos em uma relação de origem para cache para cargas de trabalho que exigem bloqueio aprimorado.

Destaques do ONTAP 9.9,1

O ONTAP 9.91,1 oferece recursos novos e aprimorados nas áreas de eficiência de storage, autenticação multifator, recuperação de desastres e muito mais. Para obter uma lista completa de novos recursos e

aprimoramentos, O que há de novo no ONTAP 9.9,1consulte .

- Segurança aprimorada para gerenciamento de acesso remoto CLI

  O suporte para hash de senha SHA512 e SSH A512 protege as credenciais da conta de administrador de agentes maliciosos que estão tentando obter acesso ao sistema.

- "Aprimoramentos de IP do MetroCluster: Suporte para clusters de 8 nós"

  O novo limite é duas vezes maior do que o anterior, fornecendo suporte para configurações MetroCluster e permitindo disponibilidade contínua de dados.

- Sincronização ativa do SnapMirror

  Oferece mais opções de replicação para backup e recuperação de desastres para grandes contêineres de dados para workloads nas.

- Maior performance da SAN

  Oferece performance de SAN até quatro vezes maior para aplicações LUN únicas, como datastores VMware, para que você possa obter alta performance em seu ambiente SAN.

- Nova opção de storage de objetos para nuvem híbrida

  Permite o uso do StorageGRID como destino do NetApp Cloud Backup Service para simplificar e automatizar o backup de seus dados ONTAP no local.

Próximas etapas

- Atualize para a versão mais recente do ONTAP
- Quando devo atualizar o ONTAP?

O que há de novo no ONTAP 9.16,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.16,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar para a versão mais recente do ONTAP, "Prepare-se para atualizar o ONTAP"consulte .

Proteção de dados

Atualização	Descrição
Suporte para backups em nuvem SnapMirror a partir de um volume migrado	A nuvem SnapMirror dá suporte a backups de volumes migrados para a nuvem usando um processo de sincronização mais eficiente. A nova funcionalidade suporta backups em nuvem SnapMirror de um volume migrado na nuvem para o mesmo ponto de extremidade de armazenamento de objetos de destino sem a necessidade de executar uma operação de linha de base novamente. Tanto o FlexVol quanto o FlexGroup volumes são compatíveis.
Suporte para migração de chave de criptografia entre gerenciadores de chaves	Ao alternar do gerenciador de chaves integrado do ONTAP para um gerenciador de chaves externo no nível do cluster, você pode usar a interface de linha de comando (CLI) do ONTAP para migrar facilmente as chaves de criptografia de um gerenciador de chaves para o outro.

Rede

Atualização	Descrição
Suporte de autenticação MD5.1X para grupos de pares BGP	O ONTAP suporta autenticação MD5 em grupos de pares BGP para proteger sessões BGP. Quando o MD5 está ativado, as sessões de BGP só podem ser estabelecidas e processadas entre pares autorizados, evitando possíveis interrupções da sessão por um ator não autorizado.
Suporte a descarga de hardware IPsec	A segurança IP (IPsec) é uma opção de segurança de dados em movimento disponível para proteger todo o tráfego IP entre um cliente e um nó ONTAP. O protocolo estava inicialmente disponível com o ONTAP 9.8 e foi implementado apenas como software. A partir do ONTAP 9.16,1, você tem a opção de descarregar determinadas operações computacionalmente intensivas, como verificações de criptografia e integridade, para uma placa de controlador de interface de rede (NIC) suportada instalada nos nós de armazenamento. O uso dessa opção de descarga de hardware pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido por IPsec.

S3 storage de objetos

Atualização	Descrição
O bucket multiprotocolo S3 suporta o upload de várias partes	Com o Multipart upload, você pode fazer o upload de um único objeto como um conjunto de peças para o bucket multiprotocolo S3.
Suporte para compartilhamento de recursos entre origens (CORS) para buckets do ONTAP S3	Desbloqueie todo o potencial de seus aplicativos da Web com o Compartilhamento de recursos entre origens (CORS). O CORS permite a interação perfeita entre aplicativos de cliente de um domínio e recursos em outro. Ao integrar o suporte do CORS, você pode capacitar seus aplicativos da Web baseados no ONTAP S3 com acesso seletivo entre origens aos seus recursos.

Atualização	Descrição
O ONTAP é compatível com a captura de snapshots dos buckets do ONTAP S3	Você pode gerar snapshots pontuais e somente leitura dos buckets do ONTAP S3. Usando o recurso snapshots S3, você pode criar snapshots manualmente ou gerá-los automaticamente por meio de políticas de snapshot. Além disso, você pode exibir, navegar e excluir snapshots S3 e restaurar o conteúdo de snapshot por meio de clientes S3.

SAN

Atualização	Descrição
Alocação de espaço NVMe habilitada por padrão	A alocação de espaço (também chamada de "perfuração" e "desmapear") é habilitada para namespaces NVMe por padrão. A desalocação de espaço permite que um host inutilize blocos de nomes para recuperar espaço. Isso melhora muito a eficiência geral de armazenamento, especialmente com sistemas de arquivos que têm alta rotatividade de dados.

Segurança

Atualização	Descrição
Conjunto elegível de comandos protegidos por regras estendidos para verificação de vários administradores	Os administradores podem criar regras de verificação de vários administradores para proteger grupos de consistência, incluindo criar, excluir e modificar operações, criar e excluir snapshots de grupos de consistência e outros comandos.
Proteção autônoma contra ransomware com aprimoramentos de AI (ARP/AI)	O ARP foi atualizado com novos recursos de AI, permitindo que a TI detete e responda a ataques de ransomware com 99% de precisão e recall. Como a IA é treinada em um conjunto de dados abrangente, não há mais um período de aprendizado para o ARP sendo executado em volumes FlexVol e o ARP/AI começa no modo ativo imediatamente. O ARP/AI também vem com uma capacidade de atualização automática para garantir proteção e resiliência constantes contra as ameaças mais recentes. O recurso ARP/AI atualmente suporta apenas nas. Embora o recurso de atualização automática exiba a disponibilidade de novos arquivos de segurança para implantação no System Manager, essas atualizações são aplicáveis apenas à proteção da carga de trabalho nas.
Suporte para criptografia em trânsito para tráfego de dados enviado de e para dispositivos de storage NVMe	O ONTAP agora oferece suporte à criptografia em trânsito para tráfego de dados enviado pela rede de e para dispositivos de storage NVMe.

Atualização	Descrição
Suporte para TLS 1,3 para comunicação de armazenamento de objetos FabricPool	O ONTAP suporta TLS 1,3 para comunicação de armazenamento de objetos FabricPool.
OAuth 2,0 para Microsoft Entra ID	O suporte do OAuth 2,0, introduzido pela primeira vez com o ONTAP 9.14,1, foi melhorado para suportar o servidor de autorização do Microsoft Entra ID (anteriormente Azure AD) com reclamações padrão do OAuth 2,0. Além disso, as reivindicações de grupo padrão do Entra ID baseadas em valores de estilo UUID são suportadas por meio de novos recursos de mapeamento de grupo e função. Também foi introduzido um novo recurso de mapeamento de funções externo que foi testado com o Entra ID, mas pode ser usado com qualquer um dos servidores de autorização suportados.

Eficiência de storage

Atualização	Descrição
Monitoramento estendido de desempenho de qtree para incluir métricas de latência e estatísticas históricas	As versões anteriores do ONTAP fornecem métricas robustas em tempo real para o uso de qtree, como operações de e/S por segundo e taxa de transferência em várias categorias, incluindo leituras e gravações. A partir do ONTAP 9.16,1, você também pode acessar estatísticas de latência em tempo real, bem como visualizar dados históricos arquivados. Essas novas funcionalidades fornecem aos administradores de storage DE TI mais insights sobre a performance do sistema e permitem a análise de tendências por períodos mais longos. Isso permite que você tome decisões mais informadas e baseadas em dados relacionadas à operação e Planejamento de seu datacenter e recursos de armazenamento em nuvem.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Suporte para distribuição de capacidade avançada FlexGroup	Quando habilitado, o balanceamento avançado de capacidade distribui dados entre os volumes membros do FlexGroup quando arquivos muito grandes crescem e consomem espaço em um volume de membro.
Suporte de mobilidade de dados SVM para migração de configurações do MetroCluster	O ONTAP agora é compatível com a migração de um par de HA que não é MetroCluster para uma configuração MetroCluster ou de uma configuração MetroCluster para um par de HA que não é MetroCluster. Não é possível migrar um SVM de uma configuração do MetroCluster para outra configuração do MetroCluster

System Manager

Atualização	Descrição
Suporte para autenticação multifator WebAuthn resistente a phishing no System Manager	O ONTAP 9.16,1 oferece suporte a logins de MFA WebAuthn, permitindo que você use chaves de segurança de hardware como um segundo método de autenticação ao fazer login no Gerenciador de sistema.
Suporte para implantações de FSX com conexão aérea	Se suas implantações do Amazon FSX for NetApp ONTAP detetarem que você está em uma região sem problemas, ir para a página de login traz para o Gerenciador de sistema, permitindo que você gerencie o FSX for ONTAP com o Gerenciador de sistema.

O que há de novo no ONTAP 9.15,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.15,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar para a versão mais recente do ONTAP, "Prepare-se para atualizar o ONTAP"consulte .

Proteção de dados

Atualização	Descrição
Aplicativos de backup do Windows e links simbólicos em estilo Unix	Quando um aplicativo de backup do Windows encontra um link simbólico de estilo Unix (link simbólico), o link é seguido e os dados reais são retornados pelo ONTAP e copiados. Começando com ONTAP 9.15,1, você também tem a opção de fazer backup do próprio link simbólico em vez dos dados para os quais ele aponta. Isso pode fornecer vários benefícios, incluindo melhor desempenho de seus aplicativos de backup. Você pode ativar o recurso usando a CLI do ONTAP ou a API REST.
O SnapMirror active Sync é compatível com implantações ativo-ativo simétricas	O SnapMirror active Sync (anteriormente SnapMirror Business Continuity) agora é compatível com implantações ativas-ativas simétricas, permitindo operações de e/S de leitura e gravação de ambas as cópias de um LUN protegido com replicação síncrona bidirecional.
Aumento do limite de volumes em um grupo de consistência usando o SnapMirror assíncrono	Os grupos de consistência que usam a proteção assíncrona do SnapMirror agora oferecem suporte a até 80 volumes no grupo de consistência.

Atualização	Descrição
Suporte para nível de privilégio de administrador para operações de API REST e CLI com grupos de consistência	As operações de CLI e API REST para grupos de consistência agora são suportadas no nível de privilégio administrativo.
Reservas persistentes para volumes virtuais VMware com cluster de failover do Windows Server	O ONTAP atualmente oferece suporte a volumes virtuais VMware (vVols) e a reservas persistentes com LUNs tradicionais. A partir do ONTAP 9.15,1, você também pode criar uma reserva persistente com uma evolução. O suporte a esse recurso é implementado nas Ferramentas do ONTAP para VMware vSphere 9. Ele só é suportado em um cluster de failover do Windows Server (WSFC), que é um grupo de máquinas virtuais do Windows em cluster.

Segurança

Atualização	Descrição
Criação e configuração de armazenamento persistente do FPolicy simplificados	Você pode criar o armazenamento persistente FPolicy e automatizar sua criação e configuração de volume ao mesmo tempo usando o `persistent-store create` comando. O comando aprimorado `persistent-store create` também permite o uso do parâmetro de modo automático, que permite que o volume cresça ou diminua em tamanho em resposta à quantidade de espaço usado.
Suporte para NFSv3 com RDMA	As configurações de NFS em RDMA agora são compatíveis com NFSv3.
O FPolicy é compatível com o protocolo NFS 4,1	O FPolicy é compatível com o protocolo NFS 4,1.
Suporte ao formato do motor Protobuf para FPolicy	O Protobuf é o mecanismo neutro em linguagem do Google para serializar dados estruturados. É menor, mais rápido e mais simples em comparação com XML, o que ajuda a melhorar o desempenho do FPolicy. Você pode usar o formato de mecanismo externo protobuf. Quando definido como protobuf, as mensagens de notificação são codificadas em forma binária usando o Google Protobuf. Antes de definir o formato do mecanismo externo para protobuf, certifique-se de que o servidor FPolicy também suporta a desserialização de protobuf.
Autorização dinâmica para conexões SSH	O ONTAP 9.15,1 fornece a estrutura inicial para autorização dinâmica, que fornece segurança aprimorada para o gerenciamento do sistema ONTAP, permitindo que você atribua uma pontuação de confiança de segurança aos usuários administradores e desafie-os com verificações de autorização adicionais quando sua atividade parecer suspeita. Você pode utilizar a autorização dinâmica como parte de uma arquitetura de segurança Zero Trust centrada em dados.

Atualização	Descrição
Suporte para TLS 1,3 para armazenamento S3, FlexCache e criptografia de peering de cluster	O TLS 1,3 tem suporte desde o ONTAP 9.11,1 para acesso de gerenciamento, mas agora é compatível com o ONTAP 9.15,1 para criptografia de peering de cluster, FlexCache e armazenamento S3. Alguns aplicativos, como o FabricPool, o armazenamento de Blobs de páginas do Microsoft Azure e a nuvem do SnapMirror, continuam limitados ao uso do TLS 1,2 para a versão 9.15.1.
Suporte a TLS para conexões NFS	O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1. O NFS sobre TLS fornece criptografia em trânsito de dados do dispositivo de storage para o cliente. O TLS é mais recente e mais conveniente do que o Kerberos, permitindo uma configuração e administração mais simples.
Conjunto elegível de comandos protegidos por regras estendidos para verificação de vários administradores	Os administradores podem criar regras de verificação de vários administradores para proteger a configuração do cluster, a exclusão LUN, a configuração do sistema, a configuração de segurança para IPsec e SAML, operações de snapshot de volume, configuração de SVM e outros comandos.
Entrega de mensagens AutoSupport usando SMTP com TLS	Embora o transporte recomendado de mensagens AutoSupport para o NetApp seja HTTPS, SMTP não criptografado também está disponível. Com o ONTAP 9.15,1, os clientes agora têm a opção de usar TLS com SMTP. O protocolo SMTPS estabelece um canal de transporte seguro, criptografando o tráfego de e-mail, bem como as credenciais opcionais do servidor de e-mail. TLS explícito é usado e, portanto, TLS é ativado após a conexão TCP ser criada. Se cópias das mensagens forem enviadas para endereços de e-mail locais, a mesma configuração será usada.

Eficiência de storage

Atualização	Descrição
Alterações no relatório de métricas de espaço de volume	Dois novos contadores foram introduzidos que mostram apenas os metadados que estão sendo usados. Além disso, vários dos contadores existentes foram ajustados para remover os metadados e exibir apenas os dados do usuário. Juntas, essas mudanças fornecem uma visão mais clara das métricas separadas nos dois tipos de dados. Os clientes podem usar esses contadores para implementar modelos de chargeback mais precisos, descontando os metadados do total e considerando apenas os dados reais do usuário.
Eficiência de storage com CPU ou processador de descarga dedicado	O ONTAP fornece eficiência de storage e compactação de dados nas plataformas AFF A70, AFF A90 e AFF A1K. Dependendo da plataforma, a compactação é realizada usando a CPU principal ou com um processador de descarga dedicado. A eficiência de storage é ativada automaticamente e não requer configuração.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Suporte de escrita FlexCache	Quando o writeback é ativado no volume do cache, as solicitações de gravação são enviadas para o cache local em vez do volume de origem, proporcionando melhor desempenho para ambientes de computação de borda e caches com cargas de trabalho com gravação intensa.
Aprimoramento do desempenho do File System Analytics	A ONTAP reforça que 5 a 8% da capacidade de um volume precisa ser livre ao ativar a análise do sistema de arquivos, atenuando possíveis problemas de desempenho para volumes e análises de sistemas de arquivos.
Chaves de criptografia do FlexClone volumes	Um volume FlexClone recebe uma chave de criptografia dedicada que é independente da chave de criptografia do FlexVol volume (host).

System Manager

Atualização	Descrição
Suporte do System Manager para configurar relações do SnapLock Vault	As relações de cofre do SnapLock podem ser configuradas usando o Gerenciador de sistema quando a origem e o destino estiverem executando o ONTAP 9.15,1 ou posterior.
Melhorias de desempenho para o painel do System Manager	As informações sobre as exibições de integridade, capacidade, rede e desempenho do System Manager incluem descrições mais completas, incluindo aprimoramentos nas métricas de desempenho que ajudam a identificar e solucionar problemas de latência ou desempenho.

Atualização

Atualização	Descrição
Suporte para migração de LIF para nó de parceiro de HA durante a atualização automatizada sem interrupções	Se a migração de LIF para o outro grupo de lotes falhar durante uma atualização automatizada sem interrupções, os LIFs serão migrados para o nó de parceiro de HA no mesmo grupo de lotes.

O que há de novo no ONTAP 9.14,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.14,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar para a versão mais recente do ONTAP, Prepare-se para atualizar o ONTAPconsulte .

Proteção de dados

Atualização	Descrição
NVE compatível com volumes raiz do SVM	Os volumes raiz da SVM podem ser criptografados usando chaves exclusivas com o NetApp volume Encryption.
Capacidade de definir o bloqueio da cópia Snapshot em cópias de retenção de longo prazo e Para reinicializar o Relógio de conformidade	Nos clusters com uma licença SnapLock, é possível definir o bloqueio de cópia Snapshot à prova de violações para cópias Snapshot com retenção de longo prazo para cópias Snapshot criadas em volumes de destino que não sejam da SnapLock SnapMirror, e o relógio de conformidade pode ser inicializado sem volumes SnapLock presentes.
O SnapMirror ative Sync suporta reservas persistentes SCIS3 e cluster de failover do Windows	SCSI3 o cluster de failover de janelas e reservas persistentes para a sincronização ativa do SnapMirror suporta vários nós que acessam um dispositivo e, ao mesmo tempo, bloqueiam o acesso a outros nós, garantindo que o cluster para diferentes ambientes de aplicativos permaneça consistente e estável.
Cópia de snapshots granular de volume com grupos de consistência	Use grupos de consistência para replicar snapshots SnapMirror assíncronos e snapshots granular de volume para os grupos de consistência de destino para uma camada extra de recuperação de desastres.
Suporte à proteção de dados assíncrona para grupos de consistência na relação de recuperação de desastres da SVM	Os SVMs configurados para recuperação de desastres da SVM podem replicar informações de grupo de consistência para o local secundário se o SVM contiver um grupo de consistência.
"Suporte assíncrono SnapMirror para alvos de fanout 20"	O número de alvos de fanout assíncronos do SnapMirror suportados em sistemas A700 e superiores aumenta de 16 para 20 quando se usa o ONTAP 9.14,1.
Criação de cache não criptografado a partir de fonte criptografada	A partir do ONTAP 9.14,0, o FlexCache suporta a criação de um volume FlexCache não criptografado a partir de uma fonte criptografada. Em versões anteriores do ONTAP, a criação do FlexCache falhou quando a origem do cache foi criptografada.
Suporte CLI para grupos de consistência	Gerenciar grupos de consistência usando a CLI do ONTAP.

Protocolos de acesso a arquivos

Atualização	Descrição
Entroncamento de sessão NFSv4,1	O entroncamento de sessão permite vários caminhos para um datastore exportado. Isso simplifica o gerenciamento e melhora o desempenho à medida que os workloads fazem a escalabilidade vertical. É especialmente apropriado em ambientes com workloads da VMware.

MetroCluster

Atualização	Descrição
Suporte a storage de objetos S3 em agregados espelhados e sem espelhamento	Habilite um servidor de storage de objetos S3 em uma SVM em um agregado espelhado ou sem espelhamento em configurações MetroCluster IP e FC.
Suporte para provisionamento de um bucket do S3 em agregados espelhados e sem espelhamento em um cluster MetroCluster	Você pode criar um bucket em um agregado espelhado ou sem espelhamento nas configurações do MetroCluster.

Para saber mais sobre os aprimoramentos de configuração de plataforma e switch para configurações do MetroCluster, consulte"ONTAP 9 Notas de versão" _ _.

S3 storage de objetos

Atualização	Descrição
O redimensionamento automático foi ativado em volumes S3 FlexGroup para eliminar a alocação excessiva de capacidade quando os intervalos são criados neles	Quando os buckets são criados ou excluídos de volumes FlexGroup novos ou existentes, os volumes são redimensionados para um tamanho mínimo necessário. O tamanho mínimo necessário é o tamanho total de todos os buckets do S3 em um volume FlexGroup.
Suporte a storage de objetos S3 em agregados espelhados e sem espelhamento	Você pode habilitar um servidor de storage de objetos S3 em uma SVM em um agregado espelhado ou sem espelhamento em configurações MetroCluster IP e FC.
Bloqueio de objetos com base nas funções dos usuários e período de retenção de bloqueio	Objetos em buckets do S3 podem ser bloqueados para não serem sobrescritos ou excluídos. A capacidade de bloquear objetos é baseada em usuários ou tempo específicos.
Configurando o acesso para grupos de usuários LDAP para oferecer suporte a serviços de diretório externo e adicionar período de validade para acesso e chaves secretas	Os administradores do ONTAP podem configurar o acesso para LDAP (Lightweight Directory Access Protocol) ou grupos de usuários do ative Directory no storage de objetos ONTAP S3, com a capacidade de habilitar a autenticação no modo de vinculação rápida LDAP. Os usuários em grupos locais ou de domínio ou grupos LDAP podem gerar seu próprio acesso e chaves secretas para clientes S3. Você pode definir um período de validade para as chaves de acesso e chaves secretas de S3 usuários. O ONTAP fornece suporte para variáveis como `$aws:username` políticas de bucket e políticas de grupo.

SAN

Atualização	Descrição
Detecção automatizada de host NVMe/TCP	Por padrão, a detecção de host de controladoras usando o protocolo NVMe/TCP é automatizada.

Atualização	Descrição
Solução de problemas e geração de relatórios no lado do host NVMe/FC	Por padrão, o ONTAP dá suporte à capacidade de hosts NVMe/FC identificarem máquinas virtuais por um identificador exclusivo e de hosts NVMe/FC monitorarem a utilização de recursos da máquina virtual. Isso aprimora a geração de relatórios e a solução de problemas no lado do host.
Priorização de host NVMe	Você pode configurar o subsistema NVMe para priorizar a alocação de recursos para hosts específicos. Host atribuído a uma alta prioridade são alocadas contagens de fila de e/S maiores e profundidades de fila maiores.

Segurança

Atualização	Descrição
Suporte para autenticação multifator Cisco DUO para usuários SSH	Os usuários SSH podem autenticar usando o Cisco DUO como um segundo fator de autenticação durante o login.
"Melhorias no suporte ao OAuth 2,0"	O ONTAP 9.14,1 estende a autenticação baseada em token e o suporte ao OAuth 2,0 inicialmente fornecido com o ONTAP 9.14,0. A autorização pode ser configurada usando o ative Directory ou LDAP com mapeamento de grupo para função. Os tokens de acesso restrito ao remetente também são suportados e protegidos com base no TLS mútuo (MTLS). Além do Auth0 e do Keycloak, o Microsoft Windows ative Directory Federation Service (ADFS) é suportado como um Provedor de identidade (IDP).
"Estrutura de autorização do OAuth 2,0"	A estrutura Open Authorization (OAuth 2,0) é adicionada e fornece autenticação baseada em token para clientes de API REST do ONTAP. Isso possibilita o gerenciamento e a administração mais seguros dos clusters do ONTAP com workflows de automação baseados em scripts de API REST ou Ansible. Os recursos padrão do OAuth 2,0 são suportados, incluindo emissor, público, validação local, introspeção remota, reivindicação de usuário remoto e suporte de proxy. A autorização do cliente pode ser configurada usando escopos OAuth 2,0 independentes ou mapeando os usuários locais do ONTAP. Os Provedores de identidade suportados (IDP) incluem Auth0 e Keycloak usando vários servidores simultâneos.
Alertas ajustáveis para Autonomous ransomware Protection	Configure o Autonomous ransomware Protection para receber notificações sempre que uma nova extensão de arquivo for detetada ou quando um ARP Snapshot for feito, recebendo aviso prévio para possíveis eventos de ransomware.
O FPolicy oferece suporte a armazenamentos persistentes para reduzir a latência	O FPolicy permite configurar um armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificação FPolicy para reduzir a latência do cliente. Configurações obrigatórias síncronas e assíncronas não são suportadas.
O FPolicy é compatível com volumes FlexCache em SMB	O FPolicy é compatível com volumes FlexCache com NFS ou SMB. Anteriormente, FPolicy não era compatível com volumes FlexCache com SMB.

Eficiência de storage

Atualização	Descrição
Rastreamento de digitalização em File System Analytics	Acompanhe a verificação de inicialização do File System Analytics com informações em tempo real sobre o progresso e a limitação.
Aumento do espaço agregado utilizável em plataformas FAS	Para plataformas FAS, a reserva WAFL para agregados maiores que 30TB TB de tamanho é reduzida de 10% para 5%, resultando em maior espaço utilizável no agregado.
Alteração no relatório de espaço físico usado em volumes TSSE	Em volumes com eficiência de storage sensível à temperatura (TSSE) ativada, a métrica da CLI da ONTAP, por relatar a quantidade de espaço usado no volume, inclui a economia de espaço obtida como resultado do TSSE. Essa métrica é refletida nos comandos volume show -físico-usado e volume show-space -físico usado. Para o FabricPool, o valor de `-physical-used` é uma combinação da camada de capacidade e da camada de performance. Para comandos específicos, veja link:https://docs.NetApp.com/US-en/ONTAP-cli-9141/volume-show.html[`volume show`(em inglês) e link:https://docs.NetApp.com/US-en/ONTAP-cli-9141/volume-show-space.html[`volume show space`(em inglês).

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Rebalanceamento Proactive FlexGroup	Os volumes do FlexGroup oferecem suporte para mover automaticamente arquivos crescentes em um diretório para um componente remoto para reduzir gargalos de e/S no componente local.
Marcação de cópias snapshot em volumes FlexGroup	Você pode adicionar, modificar e excluir tags e rótulos (comentários) para ajudar a identificar cópias snapshot e evitar a exclusão acidental de cópias snapshot em volumes FlexGroup.
Gravação diretamente na nuvem com o FabricPool	O FabricPool adiciona a capacidade de gravar dados em um volume no FabricPool para que eles sejam diretamente para a nuvem sem esperar pela verificação de disposição em categorias.
Leitura agressiva com FabricPool	O FabricPool fornece leitura agressiva de arquivos, como fluxos de filmes em volumes FabricPool, para garantir que nenhum quadro seja descartado.

Melhorias no gerenciamento de SVM

Atualização	Descrição
Suporte à mobilidade de dados SVM para migração de SVMs que contêm cotas de usuários e grupos e qtrees	A mobilidade de dados do SVM adiciona suporte à migração de SVMs que contêm cotas de usuários e grupos e qtrees.

Atualização	Descrição
Compatível com, no máximo, 400 volumes por SVM, no máximo, 12 pares de HA e pNFS com NFS 4,1 usando mobilidade de dados SVM	O número máximo de volumes compatíveis por SVM com mobilidade de dados SVM aumenta para 400, e o número de pares de HA compatíveis aumenta para 12.

System Manager

Atualização	Descrição
Suporte para failover de teste SnapMirror	Você pode usar o Gerenciador de sistema para executar ensaios de failover de teste do SnapMirror sem interromper os relacionamentos existentes do SnapMirror.
Gerenciamento de portas em um domínio de broadcast	Você pode usar o System Manager para editar ou excluir portas que foram atribuídas a um domínio de broadcast.
Capacitação de switchover não planejado automático assistido por Mediador (MAUSO)	Você pode usar o Gerenciador do sistema para ativar ou desativar o switchover não planejado Automático assistido por Mediador (MAUSO) ao executar um switchover e switchback IP MetroCluster.
Cluster e volume marcação	Você pode usar o System Manager para usar tags para categorizar clusters e volumes de maneiras diferentes, por exemplo, por finalidade, proprietário ou ambiente. Isso é útil quando há muitos objetos do mesmo tipo. Os usuários podem identificar rapidamente um objeto específico com base nas tags que foram atribuídas a ele.
Suporte aprimorado para monitoramento de grupos de consistência	O System Manager exibe dados históricos sobre o uso do grupo de consistência.
Autenticação na banda NVMe	Você pode usar o System Manager para configurar a autenticação segura, unidirecional e bidirecional entre um host e uma controladora NVMe pelos protocolos NVMe/TCP e NVMe/FC usando o protocolo de autenticação DH-HMAC-CHAP.
O suporte para gerenciamento do ciclo de vida do bucket do S3 foi estendido para o System Manager	Você pode usar o System Manager para definir regras para excluir objetos específicos em um bucket e, por meio dessas regras, expirar esses objetos de bucket.

O que há de novo no ONTAP 9.13,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.13,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar o ONTAP, Prepare-se para atualizar o ONTAPconsulte .

Proteção de dados

Atualização	Descrição
"Verificação multi-admin"	O administrador do cluster pode ativar explicitamente a verificação de vários administradores em um cluster para exigir aprovação de quorum antes que algumas operações do SnapLock sejam executadas.
"Suporte aprimorado para gerenciar grupos de consistência, incluindo movimentação de volume e geometria"	É possível mover volumes entre grupos de consistência, modificar a geometria dos grupos de consistência hierárquicos e obter insights de capacidade para grupos de consistência. O System Manager dá suporte à criação de um grupo de consistência com novos volumes nas ou namespaces NVMe.
"Restauração NDMP com SnapMirror Synchronous"	A restauração NDMP é compatível com o SnapMirror síncrono.
Aprimoramentos de sincronização ativa do SnapMirror	• "Adicione volumes a um grupo de consistência sem interrupções com uma relação de sincronização ativa do SnapMirror." • "Utilizar a restauração NDMP com a sincronização ativa do SnapMirror".
"Suporte assíncrono ao SnapMirror com um único grupo de consistência"	Os grupos de consistência dão suporte a configurações assíncronas do SnapMirror, permitindo o uso de cofres de backups do SnapMirror para grupos de consistência únicos.

Protocolos de acesso a arquivos

Atualização	Descrição
"NFSv4.x storepool suporte"	Alguns clientes consomem muitos recursos de storepool NFSv4.x levando a outros clientes NFSv4.x sendo bloqueados devido à indisponibilidade de recursos de storepool NFSv4.x. Você pode ter a opção de habilitar a negação e o bloqueio de clientes que consomem muito recurso storepool NFSv4.x em seus ambientes.

MetroCluster

Atualização	Descrição
"Transição do MetroCluster FC para o MetroCluster IP usando um switch compartilhado para storage conetado MetroCluster IP e Ethernet"	Você pode fazer a transição de um MetroCluster FC para uma configuração MetroCluster IP (ONTAP 9.8 e posterior) sem interrupções usando um switch compartilhado.
"Transições ininterruptas de uma configuração de FC MetroCluster de oito nós para uma configuração IP MetroCluster"	Você pode migrar workloads e dados de uma configuração MetroCluster FC de oito nós existente para uma nova configuração MetroCluster IP sem interrupções.

Atualização	Descrição
"Upgrades de configuração IP MetroCluster de quatro nós usando switchover e switchback"	Atualize controladores em uma configuração IP MetroCluster de quatro nós usando switchover e switchback com `system controller replace` comandos.
"O switchover não planejado automático assistido por mediador (MAUSO) é acionado para um desligamento ambiental"	Se um site desligar graciosamente devido a um desligamento ambiental, MAUSO é acionado.
"Suporte para configurações de IP MetroCluster de oito nós"	Você pode atualizar os controladores e o storage em uma configuração IP do MetroCluster de oito nós expandindo a configuração para se tornar uma configuração temporária de doze nós e removendo os grupos de DR antigos.
"Conversão de configuração IP do MetroCluster para uma configuração de switch MetroCluster de armazenamento compartilhado"	Você pode converter uma configuração IP MetroCluster para uma configuração de switch MetroCluster de armazenamento compartilhado.

Para saber mais sobre os aprimoramentos de configuração de plataforma e switch para configurações do MetroCluster, consulte"ONTAP 9 Notas de versão" _ _.

Rede

Atualização	Descrição
Suporte de hardware expandido para interconexão de cluster RDMA	O ONTAP oferece suporte a sistemas AFF A900, ASA A900 e FAS9500 para RDMA de interconexão de cluster com uma NIC de cluster de X91153A GbE, ajudando a reduzir a latência, diminuir os tempos de failover e acelerar a comunicação entre nós.
Limites de LIF de dados aumentados	O ONTAP aumenta a flexibilidade ao aumentar os limites de dimensionamento de LIF de dados para pares de HA e clusters.
Suporte IPv6 horas por dia, 7 dias por semana durante a configuração do cluster nas plataformas A800 e FAS8700	Nas plataformas A800 e FAS8700, você pode usar a CLI ONTAP para criar e configurar novos clusters em ambientes de rede somente IPv6.

S3 storage de objetos

Atualização	Descrição
Gerenciamento do ciclo de vida do bucket do S3	As ações de expiração do objeto S3 definem quando os objetos em um bucket expiram. Essa funcionalidade permite gerenciar versões de objetos para atender aos requisitos de retenção e gerenciar o storage geral de objetos do S3 com eficiência.

SAN

Atualização	Descrição
Suporte a NVMe/FC em hosts AIX	O ONTAP dá suporte ao protocolo NVMe/FC em hosts AIX. Consulte "Ferramenta de interoperabilidade do NetApp"para obter as configurações suportadas.

Segurança

Recurso	Descrição
Proteção autônoma contra ransomware	• Verifique a funcionalidade com o Autonomous ransomware Protection • Transição automática do modo de aprendizagem para o modo ativo • Suporte à FlexGroup, Incluindo análises e relatórios para volumes e operações do FlexGroup, incluindo expansão de um volume FlexGroup, conversões de FlexVol para FlexGroup e rebalanceamento do FlexGroup.
Autenticação de chave pública SSH com ative Directory	Você pode usar uma chave pública SSH como seu método de autenticação principal com um usuário do ative Directory (AD) ou usar uma chave pública SSH como seu método de autenticação secundário depois de um usuário do AD.
X,509 certificados com chaves públicas SSH	O ONTAP permite associar um certificado X,509 à chave pública SSH para uma conta, dando-lhe a segurança adicional de verificações de expiração e revogação de certificados no início de sessão SSH.
Notificação de falha de acesso ao arquivo FPolicy	O FPolicy suporta notificações para eventos de acesso negado. As notificações são geradas para a operação de arquivo falhou devido à falta de permissão, o que inclui: Falha devido a permissões NTFS, falha devido a bits de modo Unix e falha devido a ACLs NFSv4.
Autenticação multifator com TOTP (senhas únicas baseadas em tempo)	Configure contas de usuário locais com autenticação multifator usando uma senha de tempo único (TOTP). O TOTP é sempre usado como o segundo método de autenticação. Você pode usar uma chave pública SSH ou uma senha de usuário como seu método de autenticação principal.

Eficiência de storage

Atualização	Descrição
Alteração no relatório da taxa de redução de dados primários no System Manager	A taxa de redução de dados primários exibida no System Manager não inclui mais a economia de espaço de cópia Snapshot no cálculo. Ele apenas descreve a relação entre o espaço físico usado e lógico. Nas versões anteriores do ONTAP, a taxa de redução de dados primários incluiu benefícios significativos de redução de espaço das cópias Snapshot. Como resultado, quando você atualizar para ONTAP 9.13,1, você observará uma relação primária significativamente menor sendo relatada. Você ainda pode ver as taxas de redução de dados com cópias Snapshot na visualização de detalhes **capacidade**.

Atualização	Descrição
Eficiência de storage sensível à temperatura	A eficiência de storage sensível à temperatura adiciona empacotamento sequencial de blocos físicos contíguos para melhorar a eficiência de storage. Os volumes com eficiência de storage sensível à temperatura habilitada terão o empacotamento sequencial ativado automaticamente quando os sistemas forem atualizados para o ONTAP 9.13,1.
Imposição de espaço lógico	A imposição de espaço lógico é suportada em destinos SnapMirror.
Suporte aos limites de capacidade da VM de storage	Você pode definir limites de capacidade em uma VM de storage (SVM) e ativar alertas quando o SVM estiver próximo a um limite de porcentagem.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Aumento no número máximo de inodes	O ONTAP continuará a adicionar inodes automaticamente (à taxa de 1 inodes por 32 KB de espaço de volume) mesmo que o volume aumente de 680 GB. ONTAP continuará adicionando inodes até atingir o máximo de 2.147.483.632.
Suporte para especificar um tipo SnapLock durante a criação do FlexClone	Você pode especificar um dos três tipos de SnapLock, seja Compliance, Enterprise ou não SnapLock, ao criar um FlexClone de um volume de leitura/gravação.
Ative a análise do sistema de ficheiros por predefinição	Defina a análise do sistema de arquivos para ser ativada por padrão em novos volumes.
Relacionamentos de expansão da recuperação de desastres com o FlexGroup volumes	A restrição de fanout do SVM DR com volumes FlexGroup é removida. O SVM DR com FlexGroup inclui suporte para relacionamentos de fanout do SnapMirror em oito locais.
Operação de rebalanceamento de FlexGroup único	Você pode agendar uma única operação de rebalanceamento do FlexGroup para começar em uma data e hora no futuro que você especificar.
Desempenho de leitura do FabricPool	O FabricPool fornece desempenho aprimorado de leitura sequencial para workloads de um ou vários fluxos para dados residentes na nuvem e taxa de transferência em camadas. Essa melhoria pode enviar uma taxa mais alta de Gets e coloca no repositório de objetos back-end. Se você tiver armazenamentos de objetos no local, considere a capacidade de performance no serviço de armazenamento de objetos e determinar se talvez seja necessário controlar os puts do FabricPool.
Modelos de política de QoS adaptáveis	Os modelos de política de QoS adaptáveis permitem que você defina os andares de taxa de transferência no nível SVM.

Melhorias no gerenciamento de SVM

Atualização	Descrição
Mobilidade de dados do SVM	Aumenta o suporte para migração de SVMs com até 200 volumes.

Atualização	Descrição
Suporte para recriar diretórios SVM	O novo comando CLI `debug vserver refresh-vserver-dir -node node_name` recria diretórios e arquivos ausentes. Para obter mais informações e sintaxe de comandos, "A Referência de comando do ONTAP"consulte .

System Manager

A partir do ONTAP 9.12,1, o Gerenciador de sistema é integrado ao BlueXP . Saiba mais Integração do System Manager com o BlueXP sobre o .

Atualização	Descrição
Alteração no relatório da taxa de redução de dados primários	A taxa de redução de dados primários exibida no System Manager não inclui mais a economia de espaço de cópia Snapshot no cálculo. Ele apenas descreve a relação entre o espaço físico usado e lógico. Nas versões anteriores do ONTAP, a taxa de redução de dados primários incluiu benefícios significativos de redução de espaço das cópias Snapshot. Como resultado, quando você atualizar para ONTAP 9.13,1, você observará uma relação primária significativamente menor sendo relatada. Ainda é possível ver as taxas de redução de dados com cópias Snapshot na visualização de detalhes de capacidade.
Bloqueio de cópias Snapshot à prova de violações	Você pode usar o System Manager para bloquear uma cópia Snapshot em um volume que não seja da SnapLock, a fim de proteger contra ataques de ransomware.
Suporte para gerentes de chave externos	Você pode usar o System Manager para gerenciar gerenciadores de chaves externos para armazenar e gerenciar chaves de autenticação e criptografia.
Solução de problemas de hardware	Os usuários do System Manager podem visualizar representações visuais de plataformas de hardware adicionais na página "hardware", incluindo plataformas ASA e plataformas AFF Série C. O suporte para plataformas AFF Série C também está incluído nas versões de patch mais recentes do ONTAP 9.12,1, ONTAP 9.11,1 e ONTAP 9.10,1. As visualizações identificam problemas ou preocupações com as plataformas, fornecendo um método rápido para os usuários resolverem problemas de hardware.

O que há de novo no ONTAP 9.12,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.12,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar o ONTAP, Prepare-se para atualizar o ONTAPconsulte .

Proteção de dados

Atualização	Descrição
Suporte a volumes FlexVol maiores com SnapMirror Synchronous	O tamanho máximo de FlexVol volume suportado nas configurações síncronas do SnapMirror aumentou de 100 TB para 300 TB. Os clusters de origem e destino devem estar executando *ONTAP 9.12.1P2 ou posterior*.
Suporte para arquivos e tamanhos de LUN maiores no SnapMirror Synchronous	O tamanho máximo de arquivo e LUN suportado nas configurações síncronas do SnapMirror aumentou de 16 TB para 128 TB. Os clusters de origem e destino devem estar executando o ONTAP 9.12,1 P2 ou posterior.
Suporte aprimorado para grupos de consistência	• Você pode adicionar e remover volumes de um grupo de consistência, clonar um grupo de consistência (inclusive de uma cópia Snapshot). • Grupos de consistência dão suporte à marcação de aplicações para otimizar a proteção de dados e os processos de gerenciamento. • A API REST do ONTAP dá suporte à configuração de grupos de consistência com volumes NFS/SMB ou namespaces NVMe.
SnapMirror Synchronous NDO	O SnapMirror Synchronous dá suporte a operações sem interrupções (NDO) do takeover de HA e giveback, movimentação de volume e outras operações relacionadas à manutenção. Esse recurso está disponível somente nas plataformas AFF/ASA.
O ONTAP Mediator 1,5 oferece suporte à continuidade dos negócios do SnapMirror	O ONTAP Mediator 1,5 está disponível para monitorar as relações de sincronização ativa do SnapMirror.
Aprimoramentos de continuidade da sincronização ativa do SnapMirror	A sincronização ativa do SnapMirror suporta a restauração parcial de LUN a partir de instantâneos. Além disso, a sincronização ativa do SnapMirror estende a QoS para volumes que não estão na relação do SnapMirror.
Indicador de reconstrução de data warehouse para SnapMirror assíncrono	O SnapMirror Asynchronous fornece um indicador mostrando quanto tempo uma reconstrução de data warehouse leva após um ensaio de recuperação de desastres, exibindo a porcentagem concluída.
Opção SnapLock para definir o tempo de retenção mínimo "não especificado" tempo de retenção absoluto	O SnapLock inclui uma opção para definir um tempo de retenção mínimo quando o tempo de retenção absoluto é definido como "não especificado".
Cópias Snapshot à prova de violações	Você pode bloquear uma cópia Snapshot em um volume que não seja da SnapLock para proteger contra ataques de ransomware. Bloquear cópias Snapshot ajuda a garantir que elas não sejam excluídas acidentalmente ou maliciosamente.

Protocolos de acesso a arquivos

Atualização	Descrição
Desativar tipos de criptografia fracos para comunicação Kerberos	Uma nova opção de segurança SMB permite desativar RC4 e DES em favor dos tipos de criptografia AES (Advanced Encryption Standard) para comunicação baseada em Kerberos com o KDC do ative Directory (AD).
S3 acesso de cliente aos dados nas	Os clientes S3 podem acessar os mesmos dados nas que os clientes NFS e SMB sem reformatar, facilitando o atendimento de aplicações S3 que exigem dados de objeto.
Atributos estendidos do NFS	Os servidores NFS habilitados para NFSv4,2 podem armazenar e recuperar atributos estendidos NFS (xattrs) de clientes com reconhecimento xattr.
NFSv4,2 arquivos esparsos e suporte de reserva de espaço	O cliente NFSv4,2 é capaz de reservar espaço para um arquivo esparso. O espaço também pode ser desalocado e não reservado a partir de um arquivo.

MetroCluster

Atualização	Descrição
O ONTAP Mediator 1,5 é suportado em uma configuração IP MetroCluster	O ONTAP Mediator 1,5 está disponível para monitorar configurações de IP do MetroCluster.
O suporte IPsec para protocolo de host front-end (como NFS e iSCSI) está disponível nas configurações de conexão de malha do MetroCluster IP e MetroCluster.	O suporte IPsec para protocolo de host front-end (como NFS e iSCSI) está disponível nas configurações de conexão de malha do MetroCluster IP e MetroCluster.
"Recurso de comutação forçada automática do MetroCluster em uma configuração IP do MetroCluster"	Você pode habilitar o recurso de switchover forçado automático do MetroCluster em uma configuração IP do MetroCluster. Este recurso é uma extensão do recurso de switchover não planejado assistido por Mediador (MAUSO).
"S3 em um SVM em um agregado sem espelhamento em uma configuração MetroCluster IP"	Você pode habilitar o recurso de switchover forçado automático do MetroCluster em uma configuração IP do MetroCluster. Este recurso é uma extensão do recurso de switchover não planejado assistido por Mediador (MAUSO).

Para saber mais sobre os aprimoramentos de configuração de plataforma e switch para configurações do MetroCluster, consulte"ONTAP 9 Notas de versão" _ _.

Rede

Atualização	Descrição
Serviços da LIF	Você pode usar o `management-log-forwarding` serviço para controlar quais LIFs são usados para encaminhar logs de auditoria para um serviço syslog remoto

S3 storage de objetos

Atualização	Descrição
Suporte expandido para S3 ações	As seguintes ações de API do Amazon S3 são suportadas: • `CopyObject` • `UploadPartCopy` • `BucketPolicy` (OBTER, COLOCAR, EXCLUIR)

SAN

Atualização	Descrição
Maior tamanho máximo de LUN para plataformas AFF e FAS	A partir do ONTAP 9.12.1P2, o tamanho máximo de LUN suportado nas plataformas AFF e FAS aumentou de 16 TB para 128 TB.
"Limites aumentados de NVMe"	O protocolo NVMe é compatível com o seguinte: • 8K subsistemas em uma única VM de armazenamento e um único cluster • 12 clusters de nós o NVMe/FC dá suporte a 256 controladoras por porta e o NVMe/TCP dá suporte a 2K controladoras por nó.
Suporte a NVMe/TCP para autenticação segura	A autenticação segura, unidirecional e bidirecional entre um host e uma controladora NVMe é suportada por NVMe/TCP usando o protocolo de autenticação DHHMAC-CHAP.
Compatibilidade com MetroCluster IP para NVMe	O protocolo NVMe/FC é compatível com configurações MetroCluster IP de 4 nós.

Segurança

Em outubro de 2022, a NetApp implementou alterações para rejeitar transmissões de mensagens AutoSupport que não são enviadas por HTTPS com TLSv1,2 ou SMTP seguro. Para obter mais informações, "SU484: O NetApp rejeitará mensagens AutoSupport transmitidas com segurança de transporte insuficiente"consulte .

Recurso	Descrição
Aprimoramentos de interoperabilidade da proteção autônoma contra ransomware	A proteção autônoma contra ransomware está disponível para essas configurações: • Volumes protegidos com SnapMirror • SVMs protegidas com SnapMirror • SVMs habilitadas para migração (mobilidade de dados da SVM)

Recurso	Descrição
Suporte a autenticação multifator (MFA) para SSH com FIDO2 e PIV (ambos usados pelo Yubikey)	SSH MFA pode usar troca de chaves pública/privada assistida por hardware com nome de usuário e senha. Yubikey é um dispositivo de token físico que é conetado ao cliente SSH para aumentar a segurança do MFA.
Registro à prova de violação	Todos os logs internos do ONTAP são invioláveis por padrão, garantindo que as contas de administrador comprometidas não possam ocultar ações maliciosas.
Transporte TLS para eventos	Os eventos EMS podem ser enviados para um servidor syslog remoto usando o protocolo TLS, aumentando assim a proteção por cabo para o Registro de auditoria externa central.

Eficiência de storage

Atualização	Descrição
Eficiência de storage sensível à temperatura	A eficiência de storage sensível à temperatura é habilitada por padrão nos novos volumes e plataformas AFF C250, AFF C400 e AFF C800. O TSSE não está habilitado por padrão em volumes existentes, mas pode ser habilitado manualmente usando a CLI do ONTAP.
Aumento do espaço agregado utilizável	Para as plataformas All Flash FAS (AFF) e FAS500f, a reserva do WAFL para agregados maiores que 30TB TB é reduzida de 10% para 5%, resultando em maior espaço utilizável no agregado.
File System Analytics: Principais diretórios por tamanho	O File System Analytics agora identifica os diretórios em um volume que está consumindo mais espaço.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Rebalanceamento do FlexGroup	Você pode habilitar o rebalanceamento automático de volume FlexGroup sem interrupções para redistribuir arquivos entre componentes do FlexGroup. É recomendável que você não use o rebalanceamento automático do FlexGroup após uma conversão de FlexVol para FlexGroup. Em vez disso, você pode usar o recurso de movimentação de arquivos retroativos disruptivos disponível no ONTAP 9.10,1 e posterior, digitando o `volume rebalance file-move` comando. Para obter mais informações e sintaxe de comandos, "A Referência de comando do ONTAP"consulte .
Suporte ao SnapLock para SnapVault para FlexGroup volumes	Suporte ao SnapLock para SnapVault para FlexGroup volumes

Melhorias no gerenciamento de SVM

Atualização	Descrição
Melhorias na mobilidade de dados do SVM	Os administradores de cluster podem realocar, sem interrupções, uma SVM de um cluster de origem para um cluster de destino usando FAS, plataformas AFF, em agregados híbridos. O suporte ao protocolo SMB disruptivo e à proteção Autonomous ransomware foi adicionado.

System Manager

A partir do ONTAP 9.12,1, o Gerenciador de sistema é integrado ao BlueXP . Com o BlueXP , os administradores podem gerenciar a infraestrutura de multicloud híbrida a partir de um único painel de controle, mantendo o já conhecido painel do System Manager. Ao iniciar sessão no Gestor de sistema, os administradores têm a opção de aceder à interface do Gestor de sistema no BlueXP ou aceder diretamente ao Gestor de sistema. Saiba mais Integração do System Manager com o BlueXP sobre o .

Atualização	Descrição
Suporte do System Manager para SnapLock	As operações do SnapLock, incluindo inicialização do relógio de conformidade, criação de volume SnapLock e espelhamento de arquivos WORM, são compatíveis no System Manager.
Visualização de hardware de cabeamento	Os usuários do System Manager podem visualizar informações de conetividade sobre o cabeamento entre dispositivos de hardware em seu cluster para solucionar problemas de conetividade.
Suporte para autenticação multifator com o Cisco DUO ao iniciar sessão no System Manager	Você pode configurar o Cisco DUO como um provedor de identidade SAML (IDP), permitindo que os usuários se autentiquem usando o Cisco DUO quando fizerem login no Gerenciador de sistema.
Melhorias de rede do System Manager	O System Manager oferece mais controle sobre a seleção de sub-rede e porta inicial durante a criação da interface de rede. O System Manager também dá suporte à configuração de conexões NFS por RDMA.
Temas de apresentação do sistema	Os usuários do System Manager podem selecionar um tema claro ou escuro para a exibição da interface do System Manager. Eles também podem optar por padrão para o tema usado para seu sistema operacional ou navegador. Essa capacidade permite que os usuários especifiquem uma configuração mais confortável para ler a tela.
Melhorias nos detalhes da capacidade da camada local	Os usuários do System Manager podem exibir detalhes de capacidade de camadas locais específicas para determinar se o espaço está sobrecarregado, o que pode indicar que precisam adicionar mais capacidade para garantir que o nível local não fique sem espaço.
Procura melhorada	O Gerenciador do sistema tem um recurso de pesquisa aprimorado que permite que os usuários pesquisem e acessem informações de suporte relevantes e sensíveis ao contexto e o documento do produto do Gerenciador do sistema a partir do site de suporte da NetApp diretamente através da interface do Gerenciador do sistema. Isso permite que os usuários adquiram informações de que precisam para tomar as medidas apropriadas sem ter que pesquisar em vários locais no site de suporte.

Atualização	Descrição
Melhorias no provisionamento de volume	Os administradores de storage podem escolher uma política de cópia Snapshot ao criar um volume usando o System Manager, em vez de usar a política padrão.
Aumente o tamanho de um volume	Os administradores de armazenamento podem exibir o impactos no espaço de dados e na reserva de cópias Snapshot quando usam o System Manager para redimensionar um volume.
Pool de storage e Flash Pool gestão	Os administradores de storage podem usar o System Manager para adicionar SSDs a um pool de storage SSD, criar camadas locais do Flash Pool (agregado) usando unidades de alocação de pool de storage SSD e criar camadas locais do Flash Pool usando SSDs físicos.
Suporte de NFS sobre RDMA no System Manager	O System Manager suporta configurações de interface de rede para NFS por RDMA e identifica portas compatíveis com RoCE.

O que há de novo no ONTAP 9.11,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.11,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar para a versão mais recente do ONTAP, Prepare-se para atualizar o ONTAPconsulte .

Proteção de dados

Atualização	Descrição
Servidores de chaves externas de cluster	O suporte a servidores de gerenciamento de chaves externos em cluster é adicionado aos parceiros da NetApp que fornecem uma solução de servidor KMIP em cluster. Isso permite que servidores KMIP primários e secundários sejam adicionados, evitando a duplicação de dados da chave de criptografia. Para parceiros compatíveis, consulte o "Ferramenta de Matriz de interoperabilidade".

Atualização	Descrição
Política assíncrona do SnapMirror no Gerenciador de sistemas	Você pode usar o System Manager para adicionar políticas de espelhamento e cofre pré-criadas e personalizadas, exibir políticas herdadas e substituir as programações de transferência definidas em uma política de proteção ao proteger volumes e VMs de armazenamento. Você também pode usar o System Manager para editar seus relacionamentos de proteção de VM de volume e storage.  Se você estiver executando o ONTAP 9.8P12 ou uma versão de patch posterior do ONTAP 9.8, configurou o SnapMirror usando o Gerenciador de sistema e planeja atualizar para as versões do ONTAP 9.9,1 ou ONTAP 9.10,1, use o ONTAP 9.9.1P13 ou posterior e o ONTAP 9.10.1P10 ou versões de patch posteriores para sua atualização.
Restauração de diretório único da nuvem SnapMirror	Permite que os administradores de cluster no nível de privilégios de administrador executem uma única operação de restauração de diretório a partir de um endpoint de nuvem. O UUUID do endpoint de origem deve ser fornecido para identificar o endpoint de backup a partir do qual você está restaurando. Como vários backups podem usar o mesmo `cloud_endpoint_name` que o destino, o UUID associado ao backup deve ser fornecido para o comando restore. Pode utilizar o `snapmirror show` comando para obter o `source_endpoint_uuid`.
Suporte aprimorado para sincronização ativa do SnapMirror	• O SnapMirror ative Sync suporta AIX como host • O SnapMirror ative Sync suporta SnapRestore de arquivo único, permitindo que você restaure um LUN individual ou um arquivo normal em uma configuração de sincronização ativa do SnapMirror.
Ressincronização rápida da replicação de dados do SVM	A ressincronização rápida da replicação de dados do SVM fornece aos administradores de storage a capacidade de ignorar uma reconstrução completa do data warehouse e de se recuperar mais rapidamente de um ensaio de recuperação de desastres.
Compatível com a replicação de dados do SVM com o MetroCluster	A fonte SVM-DR é compatível em ambas as extremidades de uma configuração MetroCluster.
Criação de cópias Snapshot do grupo de consistência em duas fases	Na API REST, os grupos de consistência são compatíveis com um procedimento de Snapshot em duas fases, permitindo que você realize uma pré-verificação antes de confirmar o snapshot.

Protocolos de acesso a arquivos

Atualização	Descrição
Suporte TLSv1,3	O ONTAP oferece suporte ao TLS 1,3 para protocolos de gerenciamento de APIs REST e HTTPS. O TLS 1,3 não é compatível com SP/BMC ou com criptografia de peering de cluster.

Atualização	Descrição
Suporte LDAP fast bind	Se for suportado pelo servidor LDAP, você pode usar o LDAP FAST BIND para autenticar usuários de administrador do ONTAP de forma rápida e simples.

MetroCluster

Atualização	Descrição
Suporte do ONTAP Mediator 1,4	O software ONTAP Mediator versão 1,4 é suportado nas configurações MetroCluster IP.
Suporte a grupos de consistência	Os grupos de consistência são compatíveis com as configurações do MetroCluster.
"Transição de uma configuração MetroCluster FC para uma configuração AFF A250 ou FAS500f MetroCluster IP"	Você pode fazer a transição de uma configuração MetroCluster FC para uma configuração AFF A250 ou FAS500f MetroCluster IP.

Para saber mais sobre os aprimoramentos de configuração de plataforma e switch para configurações do MetroCluster, consulte"ONTAP 9 Notas de versão" _ _.

Rede

Atualização	Descrição
Protocolo de descoberta de camada de link (LLDP)	A rede do cluster suporta LLDP para permitir que o ONTAP funcione com switches de cluster que não suportam o Protocolo de detecção de Cisco (CDP).
Serviços da LIF	Os novos serviços de LIF do lado do cliente fornecem mais controle sobre quais LIFs são usados para solicitações de saída de AD, DNS, LDAP e NIS.

S3 storage de objetos

Atualização	Descrição
Suporte adicional para ações de objeto S3	As seguintes ações são suportadas pelas APIs do ONTAP: `CreateBucket` `DeleteBucket` , , `DeleteObjects`. Além disso, o ONTAP S3 oferece suporte ao controle de versão de objetos e às ações associadas ao `PutBucketVersioning`, `GetBucketVersioning` `ListBucketVersions` .

SAN

Atualização	Descrição
Failover de LIF iSCSI	O novo recurso de failover de LIF iSCSI suporta migração automática e manual de LIFs iSCSI em um failover de parceiro SFO e em um failover local. O failover de LIF iSCSI está disponível em todas as plataformas de matriz SAN (ASA).
Migração não destrutiva de LUN para namespace NVMe e de namespace NVMe para LUN	Use a CLI do ONTAP para converter no local um LUN existente em um namespace NVMe ou um Namespace NVMe existente em um LUN.

Segurança

Atualização	Descrição
Aprimoramentos de proteção autônoma contra ransomware (ARP)	O algoritmo de deteção ARP foi aprimorado para detetar ameaças adicionais de malware. Além disso, uma nova chave de licença é usada para ativar o Autonomous ransomware Protection. Para atualizações de sistemas ONTAP a partir do ONTAP 9.10,1, a chave de licença anterior ainda fornece a mesma funcionalidade.
Verificação multi-admin	Quando a verificação de vários administradores está ativada, certas operações, como a exclusão de volumes ou cópias Snapshot, podem ser executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

Eficiência de storage

Atualização	Descrição
Veja a economia de espaço físico	Quando a eficiência de storage sensível à temperatura estiver ativada em um volume, você poderá usar o comando volume show-footprint para exibir a economia de espaço físico.
Suporte do SnapLock para FlexGroup volumes	O SnapLock oferece suporte para dados armazenados no FlexGroup volumes. O suporte ao FlexGroup volumes está disponível nos modos SnapLock Compliance e SnapLock Enterprise.
Mobilidade de dados do SVM	Aumenta o número de arrays AFF compatíveis com três e adiciona suporte para relacionamentos SnapMirror quando a origem e o destino estão executando o ONTAP 9.11,1 ou posterior. O gerenciamento de chaves externas (KMIP) também é apresentado e está disponível para instalações na nuvem e no local.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Controle de atividades no nível da SVM em File System Analytics	O controle de atividade é agregado no nível do SVM, rastreando IOPS de leitura/gravação e throughput para fornecer informações instantâneas e acionáveis sobre dados.

Atualização	Descrição
Ativar atualizações de tempo de acesso ao ficheiro	Quando ativado, o tempo de acesso é atualizado no volume de origem do FlexCache apenas se a idade do tempo de acesso atual for superior à duração especificada pelo utilizador.
Eliminação assíncrona do diretório	A exclusão assíncrona está disponível para clientes NFS e SMB quando o administrador de storage concede a eles direitos sobre o volume. Quando a exclusão assíncrona está ativada, os clientes Linux podem usar o comando mv e os clientes Windows podem usar o comando Rename para excluir um diretório e movê-lo para um diretório oculto `.ontaptrashbin`.
Suporte do SnapLock para FlexGroup volumes	O SnapLock oferece suporte para dados armazenados no FlexGroup volumes. O suporte ao FlexGroup volumes está disponível nos modos SnapLock Compliance e SnapLock Enterprise. O SnapLock não dá suporte às seguintes operações no FlexGroup volumes: SnapLock para SnapVault, retenção baseada em eventos e retenção legal.

Melhorias no gerenciamento de SVM

Atualização	Descrição
Mobilidade de dados do SVM	Aumenta o número de arrays AFF compatíveis com três e adiciona suporte para relacionamentos SnapMirror quando a origem e o destino estão executando o ONTAP 9.11,1 ou posterior. O gerenciamento de chaves externas (KMIP) também é apresentado e está disponível para instalações na nuvem e no local.

System Manager

Atualização	Descrição
Gerenciar políticas assíncronas do SnapMirror	Use o System Manager para adicionar políticas de espelhamento e cofre pré-criadas e personalizadas, exibir políticas herdadas e substituir as programações de transferência definidas em uma política de proteção ao proteger volumes e VMs de armazenamento. Você também pode usar o System Manager para editar seus relacionamentos de proteção de VM de volume e storage. Se você estiver usando a versão de patch do ONTAP 9.8P12 ou posterior do ONTAP 9.8 e tiver configurado o SnapMirror usando o Gerenciador de sistema, e você planeja atualizar para as versões do ONTAP 9.9,1 ou ONTAP 9.10,1, use o ONTAP 9.9.1P13 ou posterior e o ONTAP 9.10.1P10 ou versões de patch posteriores para sua atualização.
Visualização de hardware	O recurso de visualização de hardware no Gerenciador de sistemas suporta todas as plataformas AFF e FAS atuais.
Insights de análise do sistema	Na página Insights, o System Manager ajuda a otimizar o sistema exibindo insights adicionais de capacidade e segurança e novos insights sobre a configuração de clusters e VMs de storage.

Atualização	Descrição
Melhorias de usabilidade	• Os volumes recém-criados não são compartilháveis por padrão: Você pode especificar as permissões de acesso padrão, como exportar via NFS ou compartilhar via SMB/CIFS e especificar o nível de permissão. • Simplificação DE SAN: Ao adicionar ou editar um grupo de iniciadores, os usuários do System Manager podem exibir o status da conexão dos iniciadores no grupo e garantir que os iniciadores conetados sejam incluídos no grupo para que os dados LUN possam ser acessados.
Operações avançadas de nível local (agregado)	Os administradores do System Manager podem especificar a configuração de um nível local se não quiserem aceitar a recomendação do System Manager. Além disso, os administradores podem editar a configuração RAID de um nível local existente. Se você estiver usando a versão de patch do ONTAP 9.8P12 ou posterior do ONTAP 9.8 e tiver configurado o SnapMirror usando o Gerenciador de sistema, e você planeja atualizar para as versões do ONTAP 9.9,1 ou ONTAP 9.10,1, use o ONTAP 9.9.1P13 ou posterior e o ONTAP 9.10.1P10 ou versões de patch posteriores para sua atualização.
Gerenciar logs de auditoria	Você pode usar o Gerenciador do sistema para exibir e gerenciar logs de auditoria do ONTAP.

O que há de novo no ONTAP 9.10,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.10,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar o ONTAP, Prepare-se para atualizar o ONTAPconsulte .

Proteção de dados

Atualização	Descrição
Defina o período de retenção do SnapLock até 100 anos	Em versões anteriores ao ONTAP 9.10,1, o tempo máximo de retenção com suporte é 19 de janeiro de 2071. A partir do ONTAP 9.10,1, o SnapLock Enterprise e o Compliance oferecem um tempo de retenção até 26 de outubro de 3058 e um período de retenção de até 100 anos. Políticas anteriores são automaticamente convertidas quando você estende as datas de retenção.

Atualização	Descrição
Capacidade de criar volumes SnapLock e não SnapLock no mesmo agregado	A partir do ONTAP 9.10,1, os volumes SnapLock e não SnapLock podem existir no mesmo agregado. Portanto, não é mais necessário criar um agregado SnapLock separado para volumes SnapLock.
Grupos de consistência	Organize volumes e LUNs em grupos de consistência para gerenciar políticas de proteção de dados e garantir a fidelidade da ordem de gravação de workloads em vários volumes de storage.
Arquive backups com a nuvem pública	A nuvem SnapMirror oferece suporte à disposição em camadas de backups do ONTAP em classes de storage de objetos de nuvem pública de baixo custo na AWS e no MS Azure para retenção de longo prazo.
Suporte AES para comunicação segura de canal Netlogon	Se você se conetar a controladores de domínio do Windows usando o serviço de autenticação Netlogon, poderá usar o AES (Advanced Encryption Standard) para comunicações de canal seguras.
Kerberos para autenticação de túnel de domínio SMB	A autenticação Kerberos está disponível para autenticações de túnel de domínio para o gerenciamento do ONTAP, além do NTLM. Isso permite logins mais seguros na CLI do ONTAP e na GUI do System Manager usando credenciais do ative Directory.
Vinculação de canal para maior segurança de comunicação LDAP	A vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory e serviços de nome. Isso fornece melhor proteção contra ataques homem-no-meio.

Protocolos de acesso a arquivos

Atualização	Descrição
NFS em RDMA (somente NVIDIA)	O NFS sobre RDMA utiliza adaptadores RDMA, permitindo que os dados sejam copiados diretamente entre a memória do sistema de armazenamento e a memória do sistema host, contornando as interrupções da CPU e a sobrecarga. O NFS sobre RDMA permite o uso do armazenamento GPUDirect do NVIDIA para cargas de trabalho aceleradas por GPU em hosts com GPUs NVIDIA compatíveis.

MetroCluster

Atualização	Descrição
"Configuração do endereço IP MetroCluster da camada 3 nas configurações IP do MetroCluster"	Você pode editar o endereço IP, a máscara de rede e o gateway do MetroCluster para nós em uma configuração da camada 3.
"Atualização simplificada do controlador de nós em uma configuração de MetroCluster FC"	O procedimento de atualização para o processo de atualização usando switchover e switchback foi simplificado.

Para saber mais sobre os aprimoramentos de configuração de plataforma e switch para configurações do MetroCluster, consulte"ONTAP 9 Notas de versão" _ _.

Rede

Atualização	Descrição
Interconexão de cluster RDMA	Com o sistema de armazenamento A400 ou ASA A400 e uma placa de rede de cluster X1151A, você pode acelerar cargas de trabalho de alto desempenho em um cluster de vários nós que utiliza RDMA para tráfego intra-cluster
A confirmação é necessária antes de definir o status admin como inativo para um LIF em um SVM do sistema	Isso o protege contra a remoção acidental de LIFs que são essenciais para a operação adequada do cluster. Se você tiver scripts que invocam esse comportamento na CLI, será necessário atualizá-los para contabilizar a etapa de confirmação.
Recomendações automáticas de deteção e reparo para problemas de fiação de rede	Quando um problema de acessibilidade de porta é detetado, o Gerenciador de sistema do ONTAP recomenda uma operação de reparo para resolver o problema.
Certificados IPsec (Internet Protocol Security)	As diretivas IPsec oferecem suporte a chaves pré-compartilhadas (PSKs), além de certificados de autenticação.
Políticas de serviço LIF	As políticas de firewall são obsoletas e substituídas por políticas de serviço LIF. Uma nova política de serviço NTP LIF também foi adicionada para fornecer mais controle sobre quais LIFs são usados para solicitações NTP de saída.

S3 storage de objetos

Atualização	Descrição
S3 proteção de dados de objetos, backup e recuperação de desastres	O SnapMirror S3 fornece serviços de proteção de dados para storage de objetos ONTAP S3, incluindo buckets em configurações do ONTAP S3, e backup de bucket em destinos NetApp e não NetApp.
Auditoria S3	Você pode auditar dados e eventos de gerenciamento em ambientes do ONTAP S3. A funcionalidade de auditoria do S3 é semelhante aos recursos de auditoria nas existentes, e a auditoria do S3 e nas pode coexistir em um cluster.

SAN

Atualização	Descrição
Namespace NVMe	Você pode usar a CLI do ONTAP para aumentar ou diminuir o tamanho de um namespace. Você pode usar o System Manager para aumentar o tamanho de um namespace.
Suporte a protocolo NVMe para TCP	O protocolo NVMe (non-volátil Memory Express) está disponível para ambientes SAN em uma rede TCP.

Segurança

Atualização	Descrição
Proteção autônoma contra ransomware	Com a análise de workload em ambientes nas, o Autonomous ransomware Protection alerta você sobre atividades anormais que podem indicar um ataque. O Autonomous ransomware Protection também cria backups automáticos do Snapshot quando um ataque é detetado, além da proteção existente contra cópias Snapshot programadas.
Gerenciamento de chaves de criptografia	Use o Azure Key Vault e o serviço de gerenciamento de chaves do Google Cloud Platform para armazenar, proteger e utilizar chaves do ONTAP, simplificando o gerenciamento e o acesso de chaves.

Eficiência de storage

Atualização	Descrição
Eficiência de storage sensível à temperatura	Você pode ativar a eficiência de storage sensível à temperatura usando o modo "padrão" ou o modo "eficiente" em volumes AFF novos ou existentes.
Capacidade de mover SVMs entre clusters sem interrupções	É possível realocar os SVMs entre clusters físicos do AFF, de uma origem para um destino, para balanceamento de carga, melhorias de performance, atualizações de equipamentos e migrações de data center.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Rastreamento de atividade para objetos ativos com File System Analytics (FSA)	Para melhorar a avaliação de desempenho do sistema, o FSA pode identificar objetos ativos: Arquivos, diretórios, usuários e clientes com maior tráfego e taxa de transferência.
Bloqueio global de leitura de ficheiros	Ative um bloqueio de leitura a partir de um único ponto em todos os caches e a origem; artigo afetado na migração.
Suporte NFSv4 para FlexCache	Os volumes FlexCache são compatíveis com o protocolo NFSv4.
Criar clones a partir de volumes FlexGroup existentes	Você pode criar um volume FlexClone usando volumes FlexGroup existentes.
Converta um FlexVol volume em um FlexGroup em uma fonte de recuperação de desastres da SVM	Você pode converter o FlexVol volumes em FlexGroup volumes em uma fonte de recuperação de desastre do SVM.

Melhorias no gerenciamento de SVM

Atualização	Descrição
Capacidade de mover SVMs entre clusters sem interrupções	É possível realocar os SVMs entre clusters físicos do AFF, de uma origem para um destino, para balanceamento de carga, melhorias de performance, atualizações de equipamentos e migrações de data center.

System Manager

Atualização	Descrição
Ativar o registo de telemetria de desempenho nos registos do System Manager	Os administradores podem habilitar o Registro de telemetria se tiverem problemas de desempenho com o System Manager e, em seguida, entrar em Contato com o suporte para analisar o problema.
Arquivos de licença do NetApp	Todas as chaves de licença são entregues como arquivos de licença NetApp em vez de chaves de licença individuais de 28 carateres, tornando possível licenciar vários recursos usando um arquivo.
Atualize o firmware automaticamente	Os administradores do System Manager podem configurar o ONTAP para atualizar automaticamente o firmware.
Analise as recomendações de mitigação de riscos e reconheça os riscos relatados pelo Digital Advisor	Os usuários do System Manager podem visualizar os riscos relatados pelo Digital Advisor e revisar as recomendações sobre como mitigar os riscos. A partir de 9.10.1, os usuários também podem reconhecer riscos.
Configurar a receção do administrador das notificações de eventos do EMS	Os administradores do System Manager podem configurar a forma como as notificações de eventos do sistema de Gestão de Eventos (EMS) são entregues para que sejam notificadas sobre problemas do sistema que requerem a sua atenção.
Gerenciar certificados	Os administradores do System Manager podem gerenciar autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais (integradas).
Use o System Manager para visualizar o histórico do uso da capacidade e prever necessidades futuras de capacidade	A integração entre o Digital Advisor e o System Manager permite que os administradores visualizem dados sobre tendências históricas de uso de capacidade para clusters.
Use o Gerenciador do sistema para fazer backup dos dados para o StorageGRID usando o Cloud Backup Service	Como administrador do Cloud Backup Service, você pode fazer backup no StorageGRID se tiver o Cloud Manager implantado no local. Você também pode arquivar objetos usando o Cloud Backup Service com AWS ou Azure.

Atualização	Descrição
Melhorias de usabilidade	Começando com ONTAP 9.10,1, você pode: • Atribuir políticas de QoS a LUNs em vez do volume pai (VMware, Linux, Windows) • Editar grupo de políticas de QoS LUN • Mover um LUN • Tire um LUN off-line • Execute uma atualização de imagem do Rolling ONTAP • Crie um conjunto de portas e vincule-o a um grupo • Recomendações automáticas de deteção e reparo para problemas de fiação de rede • Ative ou desative o acesso do cliente ao diretório cópia Snapshot • Calcule o espaço que pode ser recuperado antes de excluir cópias Snapshot • Acesse alterações de campo disponíveis continuamente em compartilhamentos SMB • Veja as medições da capacidade utilizando unidades de visualização mais precisas • Gerencie usuários e grupos específicos de host para Windows e Linux • Gerir as definições do AutoSupport • Redimensione volumes como uma ação separada

O que há de novo no ONTAP 9.9,1

Saiba mais sobre os novos recursos disponíveis no ONTAP 9.9,1.

Para obter detalhes sobre problemas conhecidos, limitações e avisos de atualização em versões recentes do ONTAP 9, consulte o "ONTAP 9 Notas de versão". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Saiba mais sobre o novo e aprimorado "Recursos do ONTAP MetroCluster".

Saiba mais sobre suporte novo e aprimorado para "Plataformas FAS, ASA e AFF e switches compatíveis".

Saiba mais sobre as atualizações do "API REST do ONTAP".

Para atualizar para a versão mais recente do ONTAP, Prepare-se para atualizar o ONTAPconsulte .

Proteção de dados

Atualização	Descrição
"Compatibilidade com eficiência de storage em volumes e agregados SnapLock"	As funcionalidades de eficiência de storage para volumes e agregados do SnapLock foram ampliadas para incluir compactação de dados, deduplicação entre volumes, compressão adaptável e eficiência de storage sensível à temperatura (TSSE), o que possibilita maior economia de espaço para dados WORM.
"Compatível com a configuração de diferentes políticas de Snapshot na origem e no destino da SVM DR"	As configurações de SVM DR podem usar a política de espelhamento de arquivos para configurar diferentes políticas de Snapshot na origem e no destino. Além disso, as políticas no destino não serão sobrescritas pelas na origem.
"Suporte do System Manager para SnapMirror Cloud"	A nuvem SnapMirror agora é compatível com o Gerenciador de sistemas.
SVMs habilitadas para auditoria	O número máximo de SVMs habilitadas para auditoria suportadas em um cluster foi aumentado de 50 para 400.
SnapMirror síncrono	O número máximo de pontos de extremidade síncronos SnapMirror compatíveis por par de HA aumentou de 80 para 160.
Topologia de FlexGroup SnapMirror	Os volumes FlexGroup suportam duas ou mais relações de fanout; por exemplo, A→B, A→C. tal como volumes FlexVol, o FlexGroup fanout suporta um máximo de 8 pernas de fanout e em cascata até dois níveis; por exemplo, A→B→C.

Protocolos de acesso a arquivos

Atualização	Descrição
"Referência LDAP perseguindo melhorias"	A busca por referência LDAP é suportada com assinatura e vedação LDAP, conexões TLS criptografadas e comunicações pela porta LDAPS 636.
"Suporte LDAPS em qualquer porta"	O LDAPS pode ser configurado em qualquer porta; a porta 636 permanece o padrão.
"Versões NFSv4.x ativadas por padrão"	NFSv4,0, NFSv4,1 e NFSv4,2 são ativados por padrão.
"Identificado como suporte NFSv4,2"	O controlo de acesso obrigatório (MAC) identificado como NFS é suportado quando o NFSv4,2 está ativado. Com essa funcionalidade, os servidores ONTAP NFS têm reconhecimento de MAC, armazenando e recuperando `sec_label` atributos enviados pelos clientes.

MetroCluster

Atualização	Descrição
"Suporte IP para link compartilhado na camada 3"	As configurações IP do MetroCluster podem ser implementadas com conexões back-end roteadas por IP (camada 3).
"Suporte para clusters de 8 nós"	Clusters permanentes de 8 nós são compatíveis com configurações de IP e conexão de malha. Além disso, as plataformas AFF ASA oferecem suporte a configurações de IP MCC de 8 nós.

Para saber mais sobre os aprimoramentos de configuração de plataforma e switch para configurações do MetroCluster, consulte"ONTAP 9 Notas de versão" _ _.

Rede

Atualização	Descrição
"Resiliência de clusters"	• Monitoramento e prevenção de portas para clusters sem switch de dois nós (anteriormente disponível apenas em configurações comutadas) • Failover automático de nó quando um nó não pode servir dados em sua rede de cluster • Novas ferramentas para exibir quais caminhos de cluster estão enfrentando perda de pacote
"Extensão de LIF IP virtual (VIP)"	• O número de sistema autônomo (ASN) para o protocolo de gateway de borda (BGP) suporta um inteiro não negativo de 4 bytes. • O discriminador de saída múltipla (MED) permite seleções avançadas de rota com suporte para priorização de caminho. MED é um atributo opcional na mensagem de atualização do BGP. • O VIP BGP fornece automação de rota padrão usando agrupamento de pares BGP para simplificar a configuração.

S3 storage de objetos

Atualização	Descrição
"Suporte a metadados e tags do S3"	O servidor ONTAP S3 oferece recursos avançados de automação para clientes e aplicativos S3 com suporte para metadados de objetos definidos pelo usuário e marcação de objetos.

SAN

Atualização	Descrição
Importação de LUN estrangeiro (FLI)	O aplicativo de migração de LUN SAN no site de suporte da NetApp pode ser usado para qualificar um array estrangeiro que não esteja listado na matriz de interoperabilidade FLI.
Acesso a caminho remoto NVMe-of	Se o acesso direto ao caminho for perdido no failover, a e/S remota permite que o sistema faça failover para um caminho remoto e continue o acesso aos dados.
Suporte para clusters de 12 nós em asas	Clusters de 12 nós são compatíveis com configurações AFF ASA. Os clusters do ASA podem incluir uma combinação de vários tipos de sistemas ASA.
Protocolo NVMe-of em asas	O suporte ao protocolo NVMe-of também está disponível com um sistema AFF ASA.

Atualização	Descrição
Melhorias aos grupos	• Você pode criar um grupo que consiste em grupos existentes. • Você pode adicionar uma descrição a um grupo ou iniciadores de host que serve como um alias para o grupo ou iniciador de host. • É possível mapear grupos para dois ou mais LUNs simultaneamente.
Melhoria do desempenho de LUN único	O desempenho de LUN único para AFF foi significativamente melhorado, tornando-o ideal para simplificar implantações em ambientes virtuais. Por exemplo, o A800 pode fornecer até 400% mais IOPs de leitura aleatória.

Segurança

Atualização	Descrição
Suporte para autenticação multifator com o Cisco DUO ao iniciar sessão no System Manager	A partir do ONTAP 9.9.1P3, você pode configurar o Cisco DUO como um provedor de identidade SAML (IDP), permitindo que os usuários se autentiquem usando o Cisco DUO quando fizerem login no Gerenciador de sistema.

Eficiência de storage

Atualização	Descrição
"Defina o número de arquivos para o máximo para o volume"	Automatize os máximos de arquivos com o parâmetro volume `-files-set-maximum` , eliminando a necessidade de monitorar os limites de arquivos.

Melhorias no gerenciamento de recursos de storage

Atualização	Descrição
Melhorias de gerenciamento do File System Analytics (FSA) no System Manager	O FSA fornece recursos adicionais do System Manager para pesquisa e filtragem e para tomar medidas sobre as recomendações da FSA.
Suporte para cache de pesquisa negativa	Armazena em cache um erro "arquivo não encontrado" no volume FlexCache para reduzir o tráfego de rede causado por chamadas para a origem.
Recuperação de desastres da FlexCache	Fornece migração sem interrupções de clientes de um cache para outro.
Suporte em cascata e fanout do SnapMirror para volumes FlexGroup	Fornece suporte para relacionamentos de fanout do SnapMirror Cascade e SnapMirror para volumes do FlexGroup.
Compatível com recuperação de desastres SVM para FlexGroup volumes	A compatibilidade com recuperação de desastres do SVM para FlexGroup volumes fornece redundância usando o SnapMirror para replicar e sincronizar a configuração e os dados de um SVM.
Relatórios de espaço lógico e suporte de aplicação para FlexGroup volumes	Você pode exibir e limitar a quantidade de espaço lógico consumida pelos usuários de volume do FlexGroup.

Atualização	Descrição
Suporte de acesso SMB no qtrees	O acesso SMB é compatível com qtrees em volumes FlexVol e FlexGroup com SMB habilitado.

System Manager

Atualização	Descrição
O System Manager exibe os riscos relatados pelo Digital Advisor	Use o Gerenciador do sistema para se vincular ao consultor digital da Active IQ (também conhecido como consultor digital), que relata oportunidades de reduzir riscos e melhorar a performance e a eficiência do seu ambiente de storage.
Atribua manualmente níveis locais	Os usuários do System Manager podem atribuir um nível local manualmente quando estão criando e adicionando volumes e LUNs.
Eliminação assíncrona do diretório	Os diretórios podem ser excluídos no System Manager com a funcionalidade de exclusão assíncrona de diretório de baixa latência.
Gere Playbooks do Ansible	Os usuários do System Manager podem gerar Playbooks do Ansible a partir da IU para alguns fluxos de trabalho selecionados e usá-los em uma ferramenta de automação para adicionar ou editar volumes ou LUNs repetidamente.
Visualização de hardware	Introduzido pela primeira vez no ONTAP 9.8, o recurso de visualização de hardware agora suporta todas as plataformas AFF.
Integração com o Digital Advisor	Os usuários do System Manager podem exibir casos de suporte associados ao cluster e fazer download. Eles também podem copiar os detalhes do cluster de que precisam para enviar novos casos de suporte no site de suporte da NetApp. Os usuários do System Manager podem receber alertas do Digital Advisor para informá-los quando novas atualizações de firmware estiverem disponíveis. Em seguida, eles podem baixar a imagem de firmware e carregá-la usando o System Manager.
Integração com o Cloud Manager	Os usuários do System Manager podem configurar proteção para fazer backup de dados em pontos de extremidade de nuvem pública usando o Cloud Backup Service.
Melhorias no fluxo de trabalho de provisionamento de proteção de dados	Os usuários do Gerenciador de sistema podem nomear manualmente um destino SnapMirror e um nome de grupo ao configurar a proteção de dados.
Gerenciamento aprimorado de portas de rede	A página de interfaces de rede tem recursos aprimorados para exibir e gerenciar interfaces em suas portas residenciais.
Melhorias no gerenciamento do sistema	• Suporte para grupos aninhados • Mapeie vários LUNs para um grupo em uma única tarefa e pode usar um alias WWPN para filtragem durante o processo. • Durante a criação do NVMe-of LIF, você não precisa mais selecionar portas idênticas em ambas as controladoras. • Desative portas FC com um botão de alternância para cada porta.

Atualização	Descrição
Exibição aprimorada no System Manager de informações sobre cópias Snapshot	• Os usuários do System Manager podem exibir o tamanho das cópias Snapshot e o rótulo SnapMirror. • As reservas de cópia Snapshot são definidas como zero se as cópias Snapshot estiverem desativadas.
Exibição aprimorada no System Manager sobre informações de capacidade e localização para camadas de armazenamento	• Uma nova coluna **níveis** identifica os níveis locais (agregados) em que cada volume reside. • O System Manager mostra a capacidade física usada, juntamente com a capacidade lógica usada no nível do cluster, bem como o nível do nível local (agregado). • Os novos campos de exibição de capacidade permitem monitorar a capacidade, rastrear volumes que se aproximam da capacidade ou que estão subutilizados.
Apresentar no Gestor do sistema de alertas de emergência EMS e outros erros e avisos	O número de alertas EMS recebidos em 24 horas, bem como outros erros e avisos, são apresentados no cartão de saúde do System Manager.

Alterações nos limites e padrões do ONTAP

Saiba mais sobre algumas das alterações nos limites e padrões implementados nas versões do ONTAP 9. A NetApp se esforça para ajudar seus clientes a entender os padrões mais importantes e limitar as alterações em cada versão do ONTAP.

Alterações aos padrões ONTAP

Antes de atualizar para uma nova versão do ONTAP, você deve estar ciente de quaisquer alterações nas configurações padrão do ONTAP que possam afetar sua automação ou operações de negócios.

Recurso	Alteração predefinida	Alterado no lançamento…
Auditoria nas	Os limites máximos `file-session-io-grouping-count` e `file-session-io-grouping-duration` os parâmetros aumentaram para que você possa, opcionalmente, selecionar menos notificações de eventos de auditoria nas mais consolidadas. Isso beneficia os SVMs com altas taxas de e/S, reduzindo o impacto no storage no volume de destino. NFS_FILE_SESSION_IO_GROUING_COUNT_MAX: 20000 A 120000 NFS_FILE_SESSION_IO_GROUING_DURATION_MAX: 600 A 3600	ONTAP 9.16,1

Recurso	Alteração predefinida	Alterado no lançamento…
Volumes máximos por nó para sistemas FAS	Para sistemas FAS com mais de 200GB GB de RAM por controlador, o número máximo de volumes suportados por nó aumenta de 1000 para 2500. Em versões anteriores do ONTAP, era necessária uma "Proteção de dados otimizada (DPO)" licença para aumentar o suporte ao sistema ONTAP FAS de 1000 para 2500 volumes por nó.	ONTAP 9.16,1
`vserver object-store-server user show` comando	Em versões anteriores ao ONTAP 9.15,1, o `vserver object-store-server user show` comando retornaria as chaves secretas do usuário S3. O comando não retornará mais dados de chave secreta para usuários do S3.	ONTAP 9.15,1
Auditoria nas	A configuração de auditoria nas permite reter todos os Registros de log de auditoria por padrão. Um valor revisado para o parâmetro rotate-limit garante que o log de auditoria seja dimensionado corretamente para o volume que o suporta.	ONTAP 9.15,1
Alocação de espaço	A alocação de espaço é ativada por padrão para LUNs recém-criados. A alocação de espaço foi desativada por padrão em versões anteriores do ONTAP (9.14.1 e anteriores).	ONTAP 9.15,1
Detecção automatizada de host NVMe/TCP	Por padrão, a detecção de host de controladoras usando o protocolo NVMe/TCP é automatizada.	ONTAP 9.14,1
Criptografia AES para comunicação baseada em Kerberos	A criptografia AES para autenticação é ativada por padrão para comunicação baseada em Kerberos com servidores SMB. Você pode desativar a criptografia AES manualmente se o seu ambiente não a suportar.	ONTAP 9.13,1
Agregado RAID	A partir do ONTAP 9.12,1, o controlador do sistema não será desligado por padrão após 24 horas se algum agregado for degradado. Se um utilizador alterar `raid.timeout` a opção, o controlador do sistema continuará a desligar-se após a expiração `raid.timeout` das horas.	ONTAP 9.12,1
TLS 1,1 desativado por padrão	O TLS 1,1 é desativado por padrão para novas instalações do ONTAP. Os sistemas atualizados para o ONTAP 9.12,0 e posterior que já tenham o TLS 1,1 ativado não são afetados, pois a atualização deixará o TLS 1,1 em um estado habilitado. No entanto, se você estiver atualizando clusters com o FIPS ativado, o TLS 1,1 não é compatível com FIPS a partir do ONTAP 9.11,1, portanto, o TLS 1,1 será automaticamente desativado. Quando desativado por padrão, o TLS 1,1 pode ser ativado manualmente conforme necessário.	ONTAP 9.12,0

Recurso	Alteração predefinida	Alterado no lançamento…
TLS 1,0 desativado por padrão	O TLS 1,0 é desativado por padrão para novas instalações do ONTAP. Os sistemas atualizados para o ONTAP 9.8 e posteriores que já tenham o TLS 1,0 habilitado não são afetados, pois a atualização deixará o TLS 1,0 em um estado habilitado. No entanto, se você estiver atualizando clusters com o FIPS ativado, o TLS 1,0 não é compatível com FIPS a partir do ONTAP 9.8, portanto, o TLS 1,0 será automaticamente desativado. Quando desativado por padrão, o TLS 1,0 pode ser ativado manualmente conforme necessário.	ONTAP 9,8

Alterações nos limites do ONTAP

Antes de atualizar para uma nova versão do ONTAP, você deve estar ciente de quaisquer alterações nos limites do ONTAP que possam afetar sua automação ou operações de negócios.

Recurso	Limite de alteração	Alterado no lançamento…
Monitoramento de desempenho estendido do Qtree	Você pode ativar o monitoramento de desempenho estendido para um máximo de 50.000 qtrees em um único cluster ONTAP.	ONTAP 9.16,1
Sincronização ativa do SnapMirror	O SnapMirror ative Sync suporta volumes 80 em um grupo de consistência	ONTAP 9.15,1
Assíncrono com SnapMirror	Os grupos de consistência que usam a proteção assíncrona do SnapMirror oferecem suporte a até 80 volumes em um grupo de consistência.	ONTAP 9.15,1
Análise do sistema de arquivos	Para reduzir problemas de performance, o ONTAP força que 5 a 8% da capacidade de um volume precisa estar livre ao habilitar a análise do sistema de arquivos.	ONTAP 9.15,1
Mobilidade de dados do SVM	O número máximo de volumes compatíveis por SVM com mobilidade de dados SVM aumenta para 400, e o número de pares de HA compatíveis aumenta para 12.	ONTAP 9.14,1
Rebalanceamento do FlexGroup	O tamanho mínimo de arquivo configurável para operações de rebalanceamento do FlexGroup é aumentado de 4 KB para 20 MB.	• ONTAP 9.14,1 • ONTAP 9.13.1P1 • ONTAP 9.12.1P10
Limite de tamanho de volume FlexVol e FlexGroup	O tamanho máximo de constituinte do volume FlexVol e FlexGroup suportado nas plataformas AFF e FAS é aumentado de 100 TB para 300 TB.	ONTAP 9.12.1P2

Recurso	Limite de alteração	Alterado no lançamento…
Limite de tamanho LUN	O tamanho máximo de LUN suportado nas plataformas AFF e FAS aumentou de 16 TB para 128 TB. O tamanho máximo de LUN suportado nas configurações do SnapMirror (síncronas e assíncronas) é aumentado de 16 TB para 128 TB.	ONTAP 9.12.1P2
Limite de tamanho FlexVol volume	O tamanho máximo de volume suportado nas plataformas AFF e FAS aumentou de 100 TB para 300 TB. O tamanho máximo de FlexVol volume suportado nas configurações síncronas do SnapMirror é aumentado de 100 TB para 300 TB.	ONTAP 9.12.1P2
Limite de tamanho do ficheiro	O tamanho máximo de arquivos suportados para sistemas de arquivos nas em plataformas AFF e FAS é aumentado de 16 TB para 128 TB. O tamanho máximo de arquivo suportado nas configurações síncronas do SnapMirror é aumentado de 16 TB para 128 TB.	ONTAP 9.12.1P2
Limite de volume do cluster	Aumente a capacidade dos controladores de utilizar mais plenamente a CPU e a memória e aumentar a contagem máxima de volume para um cluster de 15.000 para 30.000.	ONTAP 9.12,1
Relações SVM-DR no FlexVol volumes	Para volumes FlexVol, o número máximo de relações SVM-DR aumentou de 64 para 128 (128 SVMs por cluster).	ONTAP 9.11,1
SnapMirror síncrono	O número máximo de operações síncronas SnapMirror permitidas por par de HA aumentou de 200 para 400.	ONTAP 9.11,1
Volumes nas FlexVol	O limite do cluster para volumes nas FlexVol aumentou de 12.000 para 15.000.	ONTAP 9.10,1
Volumes de SÃO FlexVol	O limite do cluster para volumes SAN FlexVol aumentou de 12.000 para 15.000.	ONTAP 9.10,1
SVM-DR com FlexGroup volumes	• No máximo 32 relações com a SVM-DR é compatível com volumes FlexGroup. • O número máximo de volumes com suporte em um único SVM em uma relação SVM-DR é de 300, o que inclui o número de volumes FlexVol e componentes de FlexGroup. • O número máximo de constituintes num FlexGroup não pode exceder 20. • Os limites de volume do SVM-DR são 500 por nó, 1000 por cluster (incluindo volumes FlexVol e componentes de FlexGroup).	ONTAP 9.10,1
SVMs habilitadas para auditoria	O número máximo de SVMs habilitadas para auditoria suportadas em um cluster foi aumentado de 50 para 400.	ONTAP 9.9,1

Recurso	Limite de alteração	Alterado no lançamento…
SnapMirror síncrono	O número máximo de pontos de extremidade síncronos SnapMirror compatíveis por par de HA aumentou de 80 para 160.	ONTAP 9.9,1
Topologia de FlexGroup SnapMirror	Os volumes FlexGroup suportam duas ou mais relações de fanout; por exemplo, A A B, A a C. tal como os volumes FlexVol, o FlexGroup fanout suporta um máximo de 8 pernas de fanout e em cascata até dois níveis; por exemplo, A A B a C.	ONTAP 9.9,1
Transferência simultânea do SnapMirror	O número máximo de transferências simultâneas assíncronas no nível do volume aumentou de 100 para 200. As transferências de SnapMirror de nuvem para nuvem aumentaram de 32 TB para 200 TB em sistemas high-end e de 6 TB para 20 TB SnapMirror em sistemas low-end.	ONTAP 9,8
Limite de volumes do FlexVol	O espaço consumido pelos volumes FlexVol aumentou de 100 TB para 300 TB para as plataformas ASA.	ONTAP 9,8

Suporte ao lançamento do ONTAP 9

Começando com o lançamento do ONTAP 9.8, o NetApp entrega lançamentos do ONTAP duas vezes por ano civil. Embora os planos estejam sujeitos a mudanças, a intenção é entregar novos lançamentos do ONTAP no segundo e quarto trimestre de cada ano civil. Use essas informações para Planejar o período de tempo da atualização para aproveitar a versão mais recente do ONTAP.

Versão	Data de lançamento
9.16.1	Novembro de 2024
9.15.1	Maio de 2024
9.14.1	Janeiro de 2024
9.13.1	Junho de 2023
9.12.1	Fevereiro de 2023
9.11.1	Julho de 2022
9.10.1	Janeiro de 2022
9.9.1	Junho de 2021

Níveis de suporte

O nível de suporte disponível para uma versão específica do ONTAP varia dependendo de quando o software foi lançado.

Nível de suporte	Suporte completo			Suporte limitado		Suporte por autoatendimento		
Ano	1	2	3	4	5	6	7	8
Acesso à documentação online	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Suporte técnico	Sim	Sim	Sim	Sim	Sim			
Análise de causa raiz	Sim	Sim	Sim	Sim	Sim			
Downloads de software	Sim	Sim	Sim	Sim	Sim			
Atualizações de serviço (versões de patch [P-lançamentos])	Sim	Sim	Sim					
Alertas sobre vulnerabilidades	Sim	Sim	Sim					

Para atualizar para a versão mais recente do ONTAP, Atualize para a versão mais recente do ONTAPconsulte e. Quando devo atualizar o ONTAP?

Introdução e conceitos

Conceitos de ONTAP

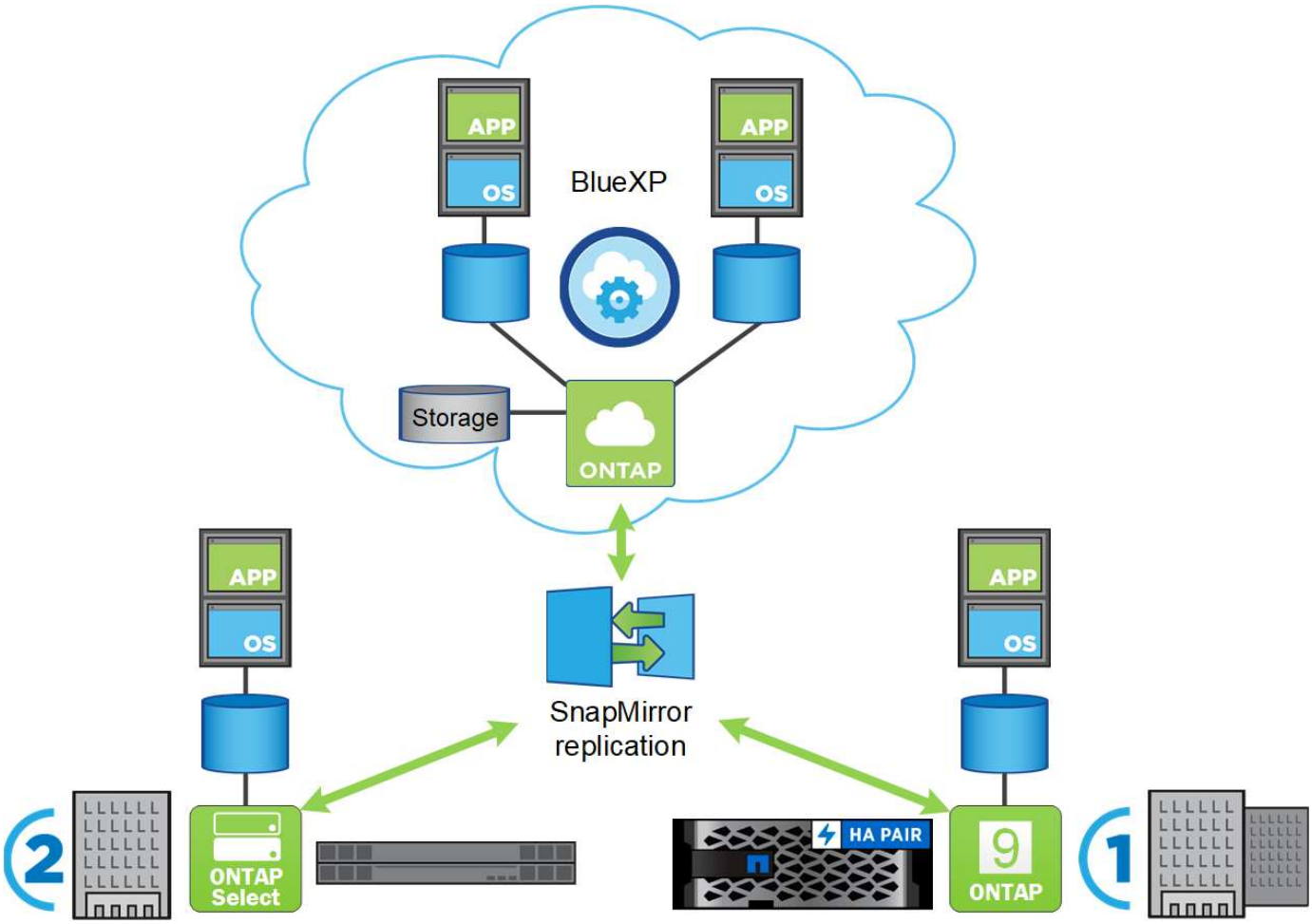
Plataformas ONTAP

O software de gerenciamento de dados ONTAP oferece storage unificado para aplicações que leem e gravam dados em bloco ou arquivo. As opções em configurações de storage variam de flash de alta velocidade a Mídia giratória de baixo preço e storage de objetos baseado na nuvem.

As implementações do ONTAP são executadas no seguinte:

- * Sistemas projetados por NetApp*: "Sistemas flash híbrido da FAS, plataformas All-Flash FAS (AFF) A-Series e C-Series e All-Flash SAN Array (ASA)"
- **Hardware de mercadoria**: "ONTAP Select"
- **Nuvens privadas, públicas ou híbridas**: "Cloud Volumes ONTAP", "Amazon FSX para NetApp ONTAP", , "Azure NetApp Files" E "Google Cloud NetApp volumes"
- **Implementações especializadas**, "Data center FlexPod" incluindo , que oferece a melhor infraestrutura convergente da categoria

Juntas, essas implementações formam a estrutura básica do *NetApp Data Fabric*, com uma abordagem comum definida por software para gerenciamento de dados e replicação rápida e eficiente entre plataformas.



Interfaces de usuário do ONTAP

O software de gerenciamento de dados ONTAP oferece várias interfaces que você pode usar para gerenciar clusters do ONTAP. Essas opções de interface oferecem diferentes níveis de acesso e funcionalidade, além de oferecer flexibilidade para gerenciar clusters do ONTAP, conforme apropriado, com base no ambiente.

Use qualquer uma dessas interfaces para administrar clusters do ONTAP e executar operações de gerenciamento de dados

Gerente do sistema da ONTAP

O ONTAP System Manager é uma interface de usuário baseada na Web que oferece uma maneira simplificada e intuitiva de gerenciar seu cluster. É possível administrar operações comuns, como configuração de storage, proteção de dados e configuração e gerenciamento de rede. O System Manager também fornece insights e monitoramento de desempenho de cluster e risco para ajudar você a reagir a problemas do cluster e se antecipar aos problemas antes que eles ocorram. "Saiba mais".

O ONTAP 9,7 marcou um momento importante para o gerente de sistema do ONTAP. Nessa versão, o NetApp forneceu duas versões do Gerenciador de sistemas ONTAP, introduzindo uma versão redesenhada, mais simplificada e intuitiva, juntamente com a versão que precedeu o ONTAP 9,7. Após o ONTAP 9,7, a versão redesenhada foi redesenhada como Gerente de sistema ONTAP e seu antecessor foi renomeado Gerente de sistema Clássico. O System Manager Classic foi atualizado pela última vez no ONTAP 9,7. Se você estiver usando o System Manager Classic, sua documentação estará "separadamente"disponível .

BlueXP

A partir do ONTAP 9.12,1, você pode usar a interface BlueXP baseada na Web para gerenciar sua infraestrutura multicloud híbrida a partir de um único painel de controle, mantendo o já conhecido dashboard do System Manager. O BlueXP permite que você crie e administre armazenamento em nuvem (por exemplo, Cloud Volumes ONTAP), use os serviços de dados do NetApp (por exemplo, backup em nuvem) e controle muitos dispositivos de armazenamento no local e na borda. A adição de sistemas ONTAP locais ao BlueXP permite que você gerencie todos os ativos de storage e dados em uma única interface. "Saiba mais".

Interface de linha de comando ONTAP

O "Interface de linha de comando ONTAP (CLI)" é uma interface baseada em texto que permite interagir com um cluster, nó, SVM e muito mais usando "comandos"o . Os comandos CLI estão disponíveis com base "tipo de função"no . Você pode acessar a CLI do ONTAP por meio de SSH ou uma conexão de console a um nó no cluster.

API REST do ONTAP

A partir do ONTAP 9.6, você pode acessar uma API RESTful que permite gerenciar e automatizar programaticamente as operações de cluster. Use a API para executar várias tarefas administrativas do ONTAP, como criar e gerenciar volumes, snapshots e agregados, além de monitorar a performance do cluster. Você pode acessar a API REST do ONTAP diretamente usando um utilitário como curl ou com qualquer linguagem de programação compatível com um CLIENTE REST, como Python, PowerShell e Java. "Saiba mais".

> ONTAPI é uma API ONTAP proprietária que precede a API REST do ONTAP. A interface ONTAPI será desativada em versões futuras do ONTAP. Se você estiver usando o ONTAPI, você deve Planejar o "Migração para a API REST do ONTAP".

Kits de ferramentas e frameworks NetApp

O NetApp fornece kits de ferramentas de cliente para linguagens e ambientes de desenvolvimento específicos que abstraem a API REST do ONTAP e facilitam a criação de código de automação. "Saiba mais".

Além desses kits de ferramentas, você pode criar e implantar código de automação usando frameworks. "Saiba mais".

Storage de cluster

A iteração atual do ONTAP foi originalmente desenvolvida para a arquitetura de armazenamento *cluster* de escalabilidade horizontal do NetApp. Essa é a arquitetura que você normalmente encontra nas implementações de data center do ONTAP. Como essa implementação exerce a maioria das capacidades do ONTAP, é um bom lugar para começar a entender os conceitos que informam a tecnologia ONTAP.

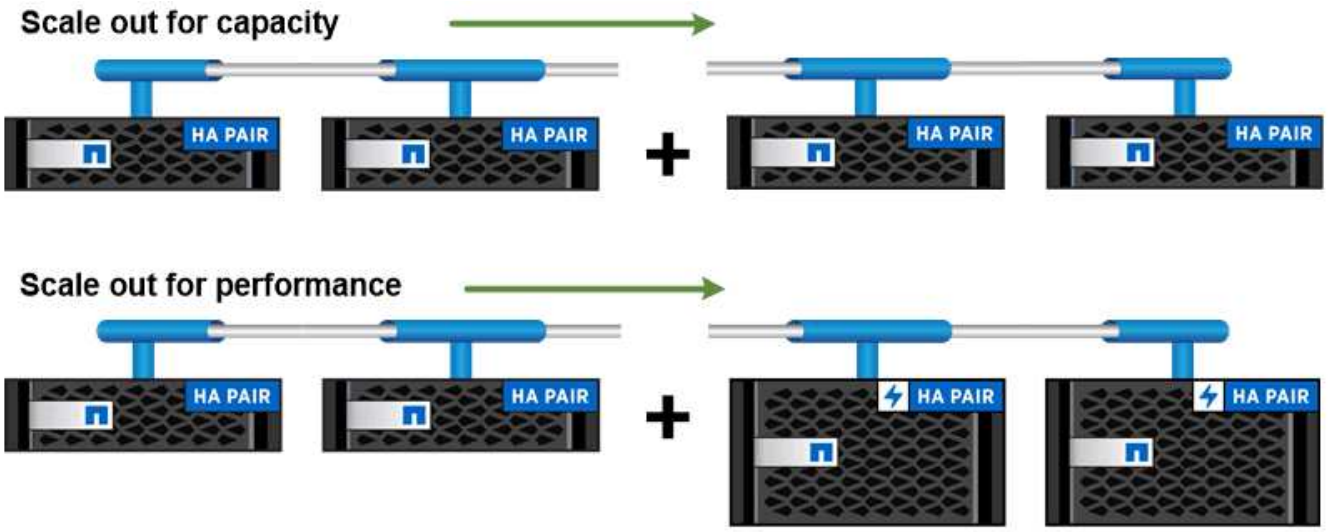
As arquiteturas de data center geralmente implantam controladores FAS ou AFF dedicados que executam o software de gerenciamento de dados ONTAP. Cada controlador, seu armazenamento, sua conetividade de rede e a instância do ONTAP em execução no controlador é chamada de *node.*

Os nós são emparelhados para alta disponibilidade (HA). Juntos, esses pares (até 12 nós para SAN, até 24 nós para nas) compõem o cluster. Os nós se comunicam uns com os outros através de uma interconexão de cluster dedicada e privada.

Dependendo do modelo da controladora, o storage de nós consiste em discos flash, unidades de capacidade ou ambos. As portas de rede no controlador fornecem acesso aos dados. Os recursos físicos de storage e conetividade de rede são virtualizados, visíveis apenas para administradores de cluster, não para clientes nas ou hosts SAN.

Os nós de um par de HA devem usar o mesmo modelo de storage array. Caso contrário, você pode usar qualquer combinação suportada de controladores. É possível fazer escalabilidade horizontal para capacidade adicionando nós com modelos de storage array semelhantes ou para obter performance adicionando nós com storage arrays mais avançados.

É claro que você também pode fazer escalabilidade vertical de todas as maneiras tradicionais, atualizando discos ou controladoras conforme necessário. A infraestrutura de storage virtualizada do ONTAP facilita a movimentação de dados sem interrupções, o que significa que você pode escalar verticalmente ou horizontalmente, sem tempo de inatividade.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

Pares de alta disponibilidade

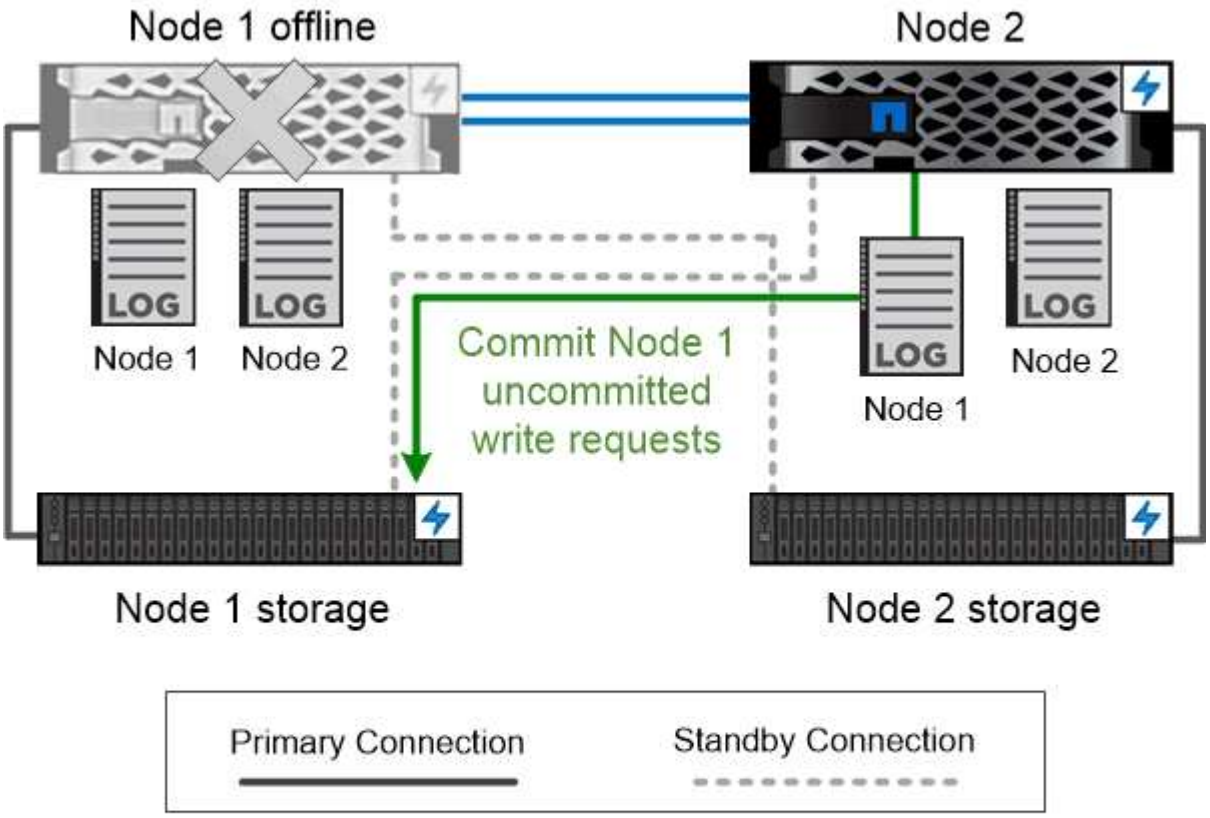
Os nós de cluster são configurados em *high-availability (HA) pairs* para tolerância de falhas e operações ininterruptas. Se um nó falhar ou se você precisar reduzir um nó para manutenção de rotina, seu parceiro pode *assumir o armazenamento e continuar a fornecer dados a partir dele. O parceiro _devolve* armazenamento quando o nó é colocado de volta na linha.

Os pares HA consistem sempre em modelos de controlador semelhantes. Normalmente, as controladoras residem no mesmo chassi com fontes de alimentação redundantes.

Os pares de HA são nós tolerantes a falhas que podem se comunicar entre si de maneiras diferentes para permitir que cada nó verifique continuamente se seu parceiro está funcionando e espelhar dados de log para a memória não volátil do outro. Quando uma solicitação de gravação é feita em um nó, ela é registrada no NVRAM em ambos os nós antes que uma resposta seja enviada de volta para o cliente ou host. No failover, o parceiro sobrevivente compromete as solicitações de gravação não confirmadas do nó com falha no disco, garantindo a consistência dos dados.

As conexões com a Mídia de armazenamento do outro controlador permitem que cada nó acesse o armazenamento do outro no caso de uma aquisição. Os mecanismos de failover de caminho de rede garantem que os clientes e hosts continuem a se comunicar com o nó sobrevivente.

Para garantir disponibilidade, você deve manter a utilização da capacidade de performance em qualquer nó em 50% para acomodar o workload adicional no caso de failover. Pelo mesmo motivo, você pode querer configurar não mais de 50% do número máximo de interfaces de rede virtual nas para um nó.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

Takeover e giveback em implementações virtualizadas de ONTAP

O storage não é compartilhado entre nós em implementações virtualizadas do ONTAP "sem nada", como o Cloud Volumes ONTAP para AWS ou ONTAP Select. Quando um nó cai, seu parceiro continua fornecendo dados de uma cópia espelhada síncrona dos dados do nó. Ele não assume o storage do nó, apenas sua função de fornecimento de dados.

AutoSupport e consultor digital

O ONTAP oferece monitoramento e geração de relatórios de sistemas orientados por inteligência artificial por meio de um portal da Web e por meio de um aplicativo móvel. O componente AutoSupport do ONTAP envia telemetria que é analisada pelo consultor digital da Active IQ (também conhecido como consultor digital).

O Digital Advisor permite otimizar sua infraestrutura de dados em toda a nuvem híbrida global, fornecendo análises preditivas práticas e suporte proativo por meio de um portal baseado na nuvem e aplicativo móvel. Insights e recomendações orientados por dados do consultor digital estão disponíveis para todos os clientes da NetApp com um contrato de SupportEdge ativo (os recursos variam de acordo com o produto e a camada de suporte).

Aqui estão algumas coisas que você pode fazer com o Digital Advisor:

- Planejar atualizações. O consultor digital identifica problemas no seu ambiente que podem ser resolvidos ao atualizar para uma versão mais recente do ONTAP e o componente do consultor de atualização ajuda você a Planejar uma atualização bem-sucedida.
- Veja o bem-estar do sistema. Seu painel do Digital Advisor relata quaisquer problemas de bem-estar e ajuda você a corrigir esses problemas. Monitore a capacidade do sistema para garantir que você nunca fique sem espaço de armazenamento.
- Gerenciar a performance. O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no System Manager. Identifique problemas de configuração e sistema que estejam afetando a performance.
- Maximizar a eficiência: Visualize as métricas de eficiência de storage e identifique maneiras de armazenar mais dados em menos espaço.
- Ver inventário e configuração. O Digital Advisor exibe o inventário completo e as informações de configuração de software e hardware. Veja quando os contratos de serviço estão expirando para garantir que você permaneça coberto.

Informações relacionadas

"Documentação do NetApp: Consultor digital"

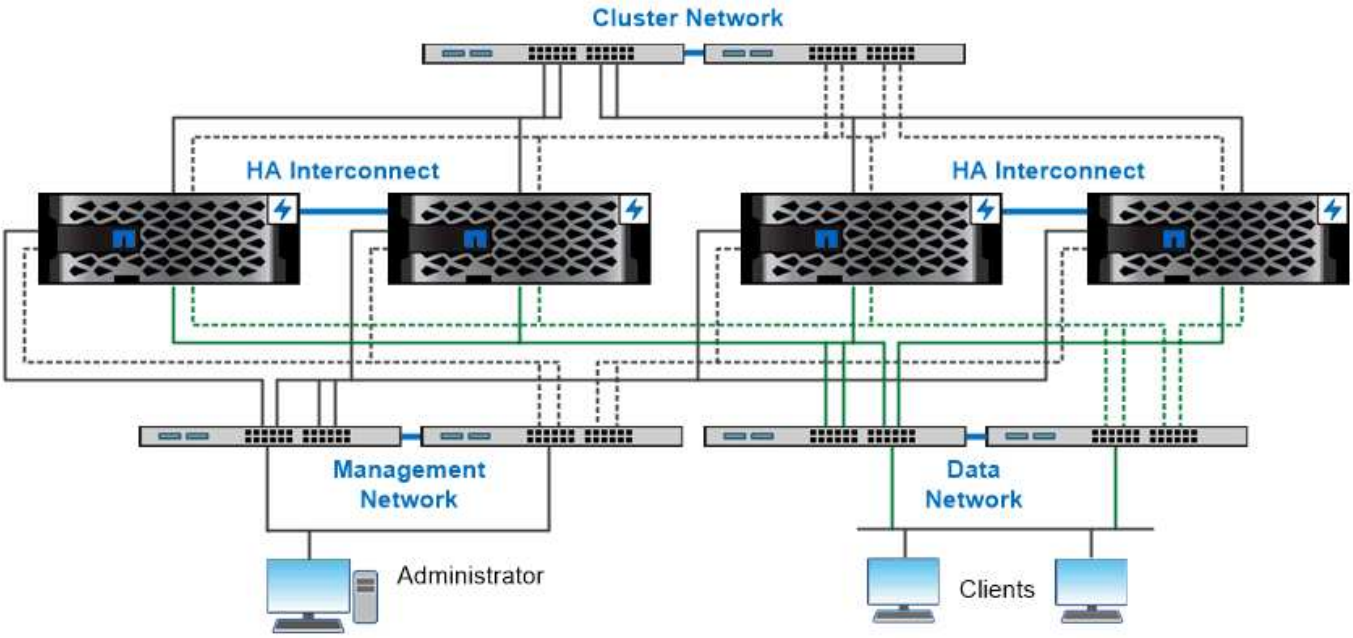
"Inicie o Digital Advisor"

"Serviços da SupportEdge"

Arquitetura de rede

Visão geral da arquitetura de rede

A arquitetura de rede para uma implementação de data center ONTAP normalmente consiste em uma interconexão de cluster, uma rede de gerenciamento para administração de cluster e uma rede de dados. Os NICs (placas de interface de rede) fornecem portas físicas para conexões Ethernet. HBAs (adaptadores de barramento de host) fornecem portas físicas para conexões FC.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

Portas lógicas

Além das portas físicas fornecidas em cada nó, você pode usar *portas lógicas* para gerenciar o tráfego de rede. As portas lógicas são grupos de interface ou VLANs.

Grupos de interfaces

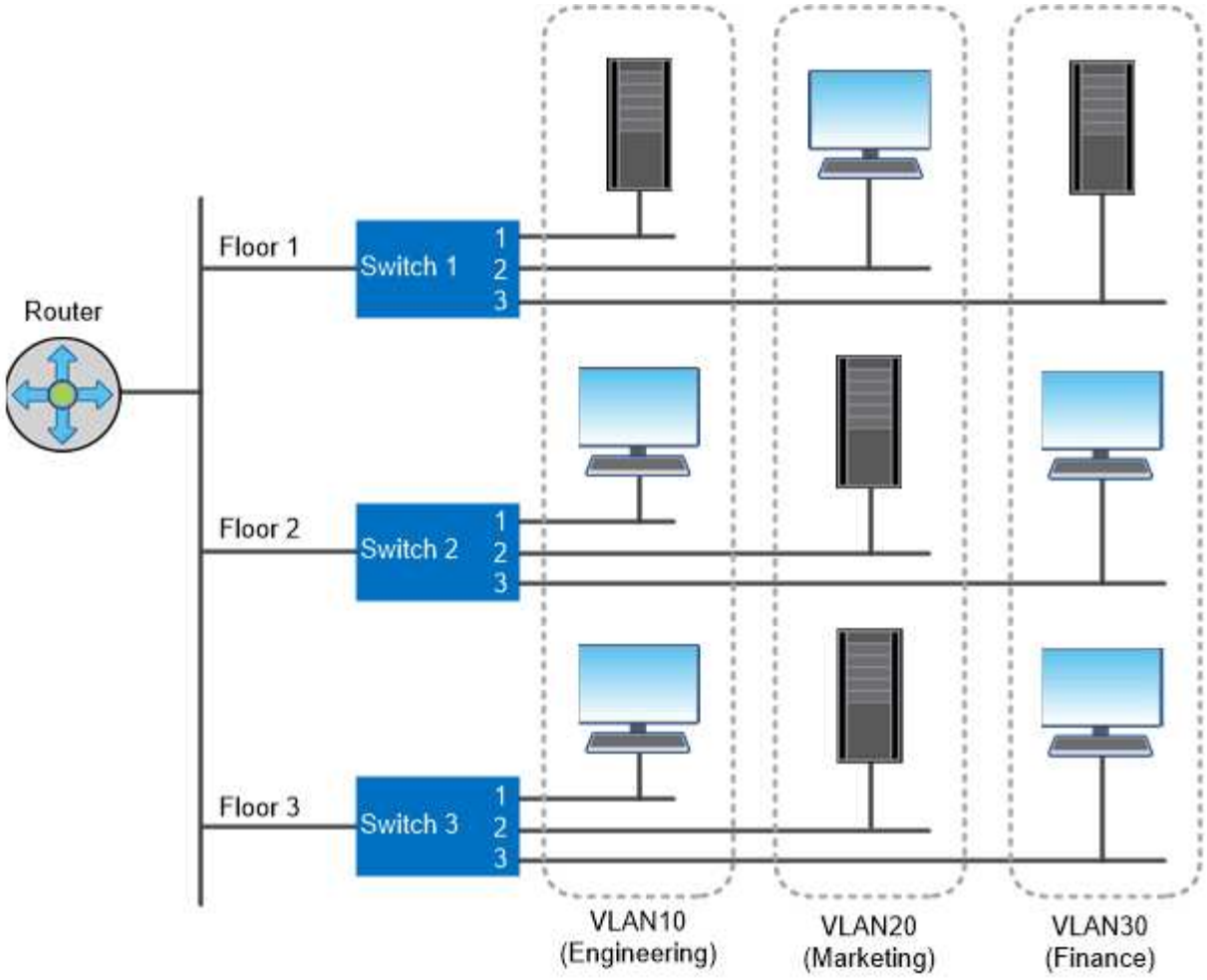
Grupos de interface combinam várias portas físicas em uma única "porta de tronco" lógica. Você pode querer criar um grupo de interfaces que consiste em portas de NICs em diferentes slots PCI para garantir que uma falha de slot reduza o tráfego essencial para os negócios.

Um grupo de interfaces pode ser multimodo, monomodo ou dinâmico. Cada modo oferece diferentes níveis de tolerância a falhas. Você pode usar qualquer um dos tipos de grupo de interface multimodo para equilibrar o tráfego de rede.

VLANs

VLANs separe o tráfego de uma porta de rede (que pode ser um grupo de interfaces) em segmentos lógicos definidos em uma base de porta de switch, em vez de em limites físicos. As *end-stations* pertencentes a uma VLAN estão relacionadas por função ou aplicação.

Você pode agrupar estações finais por departamento, como Engenharia e Marketing, ou por projeto, como release1 e release2. Como a proximidade física das estações finais é irrelevante em uma VLAN, as estações finais podem ser geograficamente remotas.



You can use VLANs to segregate traffic by department.

Suporte para tecnologias de rede padrão do setor

O ONTAP é compatível com todas as principais tecnologias de rede padrão do setor. As principais tecnologias incluem IPspaces, balanceamento de carga DNS e traps SNMP.

Domínios de broadcast, grupos de failover e sub-redes são descritos em Failover de caminho nas.

IPspaces

Você pode usar um *IPspace* para criar um espaço de endereço IP distinto para cada servidor de dados virtual em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Um provedor de serviços, por exemplo, poderia configurar diferentes IPspaces para locatários usando os mesmos endereços IP para acessar um cluster.

Balanceamento de carga DNS

Você pode usar *DNS load balancing* para distribuir o tráfego de rede do usuário entre as portas disponíveis. Um servidor DNS seleciona dinamicamente uma interface de rede para o tráfego com base no número de clientes montados na interface.

Traps SNMP

Você pode usar *SNMP traps* para verificar periodicamente se há limites operacionais ou falhas. Os traps SNMP capturam informações de monitoramento do sistema enviadas assincronamente de um agente SNMP para um gerenciador SNMP.

Conformidade com FIPS

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode ativar e desativar o modo SSL FIPS, definir protocolos SSL globalmente e desativar quaisquer cifras fracas, como RC4.

Visão geral da RDMA

As ofertas de acesso remoto à memória direta (RDMA) da ONTAP são compatíveis com cargas de trabalho sensíveis à latência e de alta largura de banda. O RDMA permite que os dados sejam copiados diretamente entre a memória do sistema de armazenamento e a memória do sistema host, contornando as interrupções da CPU e a sobrecarga.

NFS sobre RDMA

A partir do ONTAP 9.10,1, você pode configurar "NFS sobre RDMA" para habilitar o uso do armazenamento GPUDirect do NVIDIA para cargas de trabalho aceleradas por GPU em hosts com GPUs NVIDIA compatíveis.

Interconexão de cluster RDMA

A interconexão de cluster RDMA reduz a latência, diminui os tempos de failover e acelera a comunicação entre nós em um cluster.

A partir do ONTAP 9.10,1, o RDMA de interconexão de cluster é suportado para determinados sistemas de hardware quando usado com placas de rede de cluster X1151A. A partir do ONTAP 9.13,1, as placas de rede X91153A também suportam RDMA de interconexão de cluster. Consulte a tabela para saber quais sistemas são suportados em diferentes versões do ONTAP.

Sistemas	Versões de ONTAP compatíveis
• AFF A400 • ASA A400	ONTAP 9.10,1 e posterior
• AFF A900 • ASA A900 • FAS9500	ONTAP 9.13,1 e posterior

Dada a configuração apropriada do sistema de armazenamento, nenhuma configuração adicional é necessária para usar a interconexão RDMA.

Protocolos do cliente

O ONTAP dá suporte a todos os principais protocolos de cliente padrão do setor: NFS, SMB, FC, FCoE, iSCSI, NVMe e S3.

NFS

NFS é o protocolo de acesso a arquivos tradicional para sistemas UNIX e LINUX. Os clientes podem acessar arquivos em volumes ONTAP usando os seguintes protocolos.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- PNFS

Você pode controlar o acesso a arquivos usando permissões de estilo UNIX, permissões de estilo NTFS ou uma combinação de ambos.

Os clientes podem acessar os mesmos arquivos usando os protocolos NFS e SMB.

SMB

SMB é o protocolo tradicional de acesso a arquivos para sistemas Windows. Os clientes podem acessar arquivos em volumes ONTAP usando os protocolos SMB 2,0, SMB 2,1, SMB 3,0 e SMB 3.1.1. Assim como no NFS, uma combinação de estilos de permissão é compatível.

O SMB 1,0 está disponível, mas desativado por padrão no ONTAP 9.3 e versões posteriores.

FC

Fibre Channel é o protocolo original de bloco em rede. Em vez de arquivos, um protocolo de bloco apresenta um disco virtual inteiro a um cliente. O protocolo FC tradicional usa uma rede FC dedicada com switches FC especializados e exige que o computador cliente tenha interfaces de rede FC.

Um LUN representa o disco virtual e um ou mais LUNs são armazenados em um volume ONTAP. O mesmo LUN pode ser acessado através dos protocolos FC, FCoE e iSCSI, mas vários clientes só podem acessar o mesmo LUN se fizerem parte de um cluster que evite colisões de gravação.

FCoE

O FCoE é basicamente o mesmo protocolo que o FC, mas usa uma rede Ethernet de nível de data center em vez do transporte FC tradicional. O cliente ainda requer uma interface de rede específica para FCoE.

ISCSI

ISCSI é um protocolo de bloco que pode ser executado em redes Ethernet padrão. A maioria dos sistemas operacionais cliente oferece um iniciador de software que é executado em uma porta Ethernet padrão. O iSCSI é uma boa escolha quando você precisa de um protocolo de bloco para um aplicativo específico, mas não tem rede FC dedicada disponível.

NVMe/FC e NVMe/TCP

O NVMe, o protocolo de bloco mais recente, foi projetado especificamente para funcionar com storage baseado em flash. Ele oferece sessões dimensionáveis, uma redução significativa na latência e um aumento no paralelismo, o que o torna adequado para aplicações de baixa latência e alta taxa de transferência, como bancos de dados e análises in-memory.

Diferentemente do FC e iSCSI, o NVMe não usa LUNs. Em vez disso, ele usa namespaces, que são armazenados em um volume ONTAP. Os namespaces NVMe podem ser acessados somente pelo protocolo NVMe.

S3

A partir do ONTAP 9.8, é possível habilitar um servidor do Serviço de armazenamento simples (S3) do ONTAP em um cluster do ONTAP, permitindo que você forneça dados no armazenamento de objetos usando buckets do S3.

O ONTAP dá suporte a dois cenários de caso de uso no local para fornecer storage de objetos S3:

- Disposição do FabricPool em um bucket no cluster local (disposição em um bucket local) ou cluster remoto (camada de nuvem).
- S3 acesso de aplicativo cliente a um bucket no cluster local ou em um cluster remoto.

> ⓘ O ONTAP S3 é apropriado se você quiser recursos de S3 em clusters existentes sem hardware e gerenciamento adicionais. Para implantações maiores de 300TB TB, o software NetApp StorageGRID continua a ser a principal solução da NetApp para storage de objetos. Saiba mais "StorageGRID"sobre .

Discos e agregados

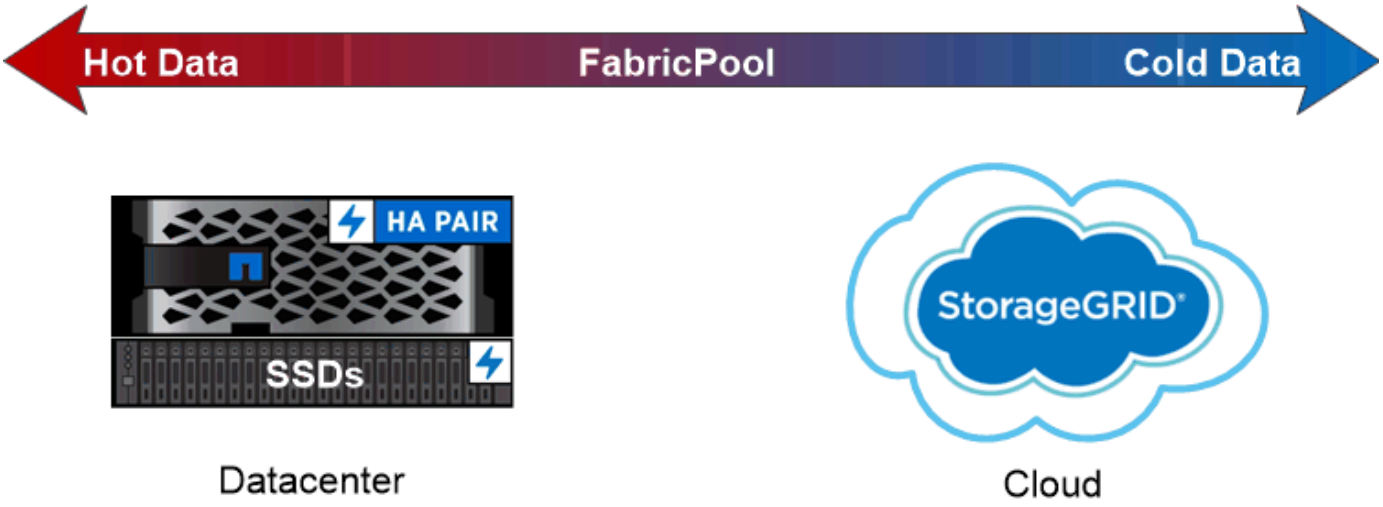
Visão geral de discos e camadas locais (agregados)

Você pode gerenciar o storage físico do ONTAP usando o Gerenciador do sistema e a CLI. Você pode criar, expandir e gerenciar camadas locais (agregados), trabalhar com camadas locais (agregados) do Flash Pool, gerenciar discos e gerenciar políticas de RAID.

Quais são os níveis locais (agregados)

Níveis locais (também chamados de *agregados*) são contentores para os discos gerenciados por um nó. Use as camadas locais para isolar workloads com demandas de desempenho diferentes, categorizar dados com padrões de acesso diferentes ou separar dados para fins regulatórios.

- Para aplicações essenciais aos negócios que precisam da menor latência possível e da maior performance possível, você pode criar um nível local que consiste inteiramente de SSDs.
- Para categorizar dados com diferentes padrões de acesso, você pode criar um *nível local híbrido*, implantando flash como cache de alto desempenho para um conjunto de dados em funcionamento, ao mesmo tempo em que usa HDDs de baixo custo ou storage de objetos para dados acessados com menos frequência.
  - Um *Flash Pool* consiste em SSDs e HDDs.
  - Um *FabricPool* consiste em um nível local totalmente SSD com um armazenamento de objetos anexado.
- Se você precisar separar os dados arquivados de dados ativos para fins regulatórios, poderá usar um nível local que consiste em HDDs de capacidade ou uma combinação de HDDs de desempenho e capacidade.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

Trabalhando com camadas locais (agregados)

Você pode executar as seguintes tarefas:

- "Gerenciar camadas locais (agregados)"
- "Gerenciar discos"
- "Gerenciar configurações RAID"
- "Gerenciar camadas do Flash Pool"

Você executa essas tarefas se as seguintes tarefas forem verdadeiras:

- Você não quer usar uma ferramenta de script automatizado.
- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você tem uma configuração do MetroCluster e segue os procedimentos descritos "MetroCluster"na documentação para configuração inicial e diretrizes para camadas locais (agregados) e gerenciamento de disco.

Informações relacionadas

- "Gerenciar categorias de nuvem do FabricPool"

Camadas locais (agregados) e grupos RAID

As tecnologias RAID modernas protegem contra falhas de disco reconstruindo os dados de um disco com falha em um disco sobressalente. O sistema compara as informações de índice em um "disco de paridade" com os dados nos restantes discos íntegros para reconstruir os dados em falta, tudo sem tempo de inatividade ou um custo significativo de desempenho.

Um nível local (agregado) consiste em um ou mais *grupos RAID*. O *tipo RAID* do nível local determina o

número de discos de paridade no grupo RAID e o número de falhas de disco simultâneas que a configuração RAID protege contra.

O tipo RAID padrão, RAID-DP (paridade RAID-dupla), requer dois discos de paridade por grupo RAID e protege contra a perda de dados no caso de dois discos falharem ao mesmo tempo. Para RAID-DP, o tamanho do grupo RAID recomendado está entre 12 e 20 HDDs e entre 20 e 28 SSDs.

Você pode espalhar o custo total dos discos de paridade criando grupos RAID na extremidade mais alta da recomendação de dimensionamento. Esse é especialmente o caso dos SSDs, que são muito mais confiáveis do que as unidades de capacidade. Para camadas locais que usam HDDs, você deve equilibrar a necessidade de maximizar o storage em disco em comparação a fatores de compensação, como o tempo de reconstrução mais longo necessário para grupos RAID maiores.

Camadas locais espelhadas e sem espelhamento (agregados)

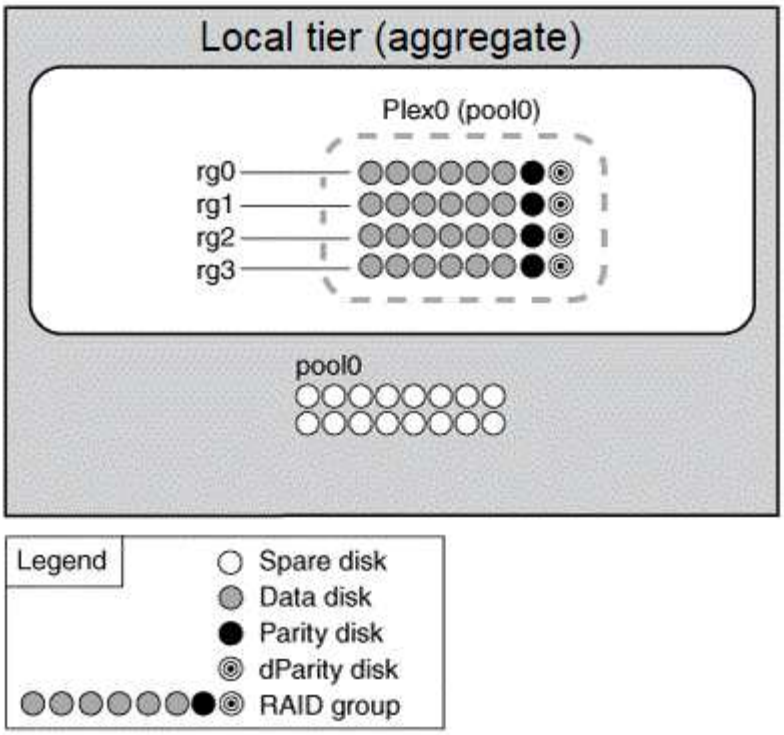
O ONTAP tem um recurso opcional chamado *SyncMirror* que você pode usar para espelhar sincronamente dados de nível local (agregado) em cópias, ou *plexes*, armazenados em diferentes grupos RAID. Os plexes garantem contra a perda de dados se mais discos falharem do que o tipo RAID protege contra, ou se houver perda de conetividade com discos do grupo RAID.

Quando você cria um nível local com o System Manager ou usando a CLI, você pode especificar que o nível local é espelhado ou sem espelhamento.

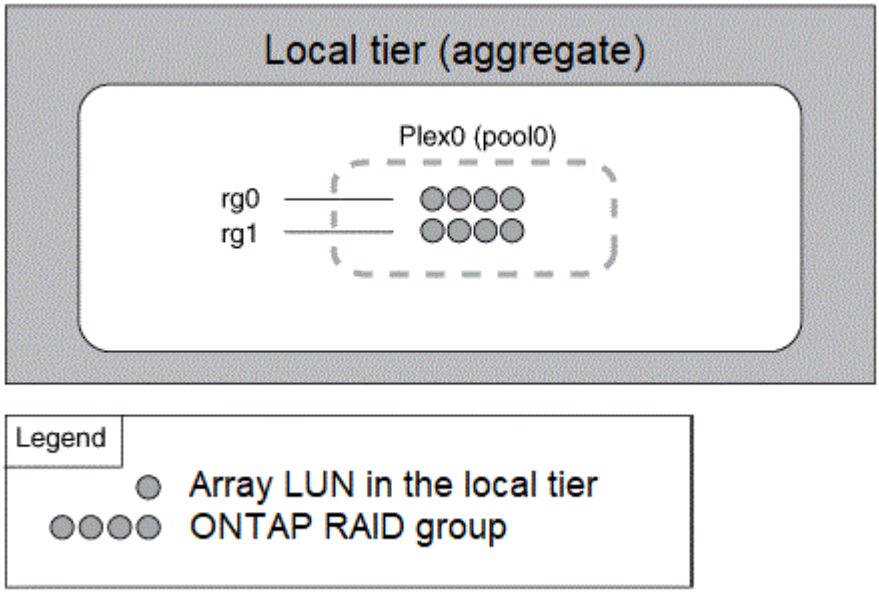
Como os agregados (camadas locais sem espelhamento) funcionam

Se você não especificar que as camadas locais são espelhadas, elas serão criadas como camadas locais sem espelhamento (agregados). Os níveis locais não espelhados têm apenas um *Plex* (uma cópia de seus dados), que contém todos os grupos RAID pertencentes a esse nível local.

O diagrama a seguir mostra um nível local sem espelhamento composto de discos, com seu único Plex. O nível local tem quatro grupos RAID: rg0, RG1, RG2 e rg3. Cada grupo RAID tem seis discos de dados, um disco de paridade e um disco de paridade (paridade dupla). Todos os discos usados pelo nível local vêm do mesmo pool, "'pool0".



O diagrama a seguir mostra um nível local sem espelhamento com LUNs de array, com um Plex. Ele tem dois grupos RAID, rg0 e RG1. Todos os LUNs de array usados pelo nível local vêm do mesmo pool, "'pool0"".



Como funcionam os agregados (camadas locais espelhadas)

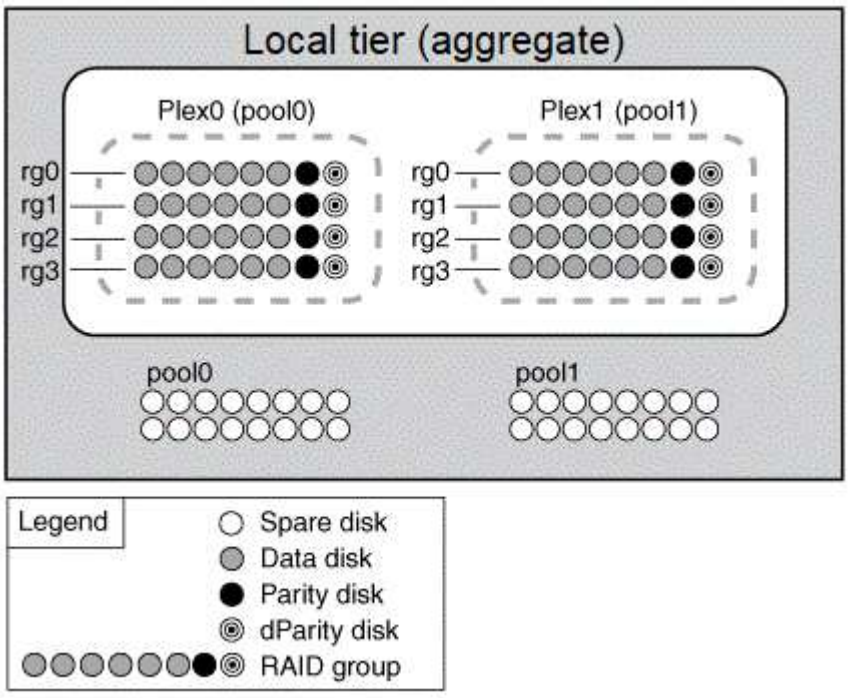
Agregados espelhados têm dois *plexes* (cópias de seus dados), que usam a funcionalidade SyncMirror para duplicar os dados para fornecer redundância.

Ao criar um nível local, você pode especificar que ele é um nível local espelhado. Além disso, você pode adicionar um segundo Plex a um nível local sem espelhamento existente para torná-lo um nível espelhado. Utilizando a funcionalidade SyncMirror, o ONTAP copia os dados no Plex original (plex0) para o novo Plex (plex1). Os plexos são separados fisicamente (cada Plex tem seus próprios grupos RAID e seu próprio pool), e os plexos são atualizados simultaneamente.

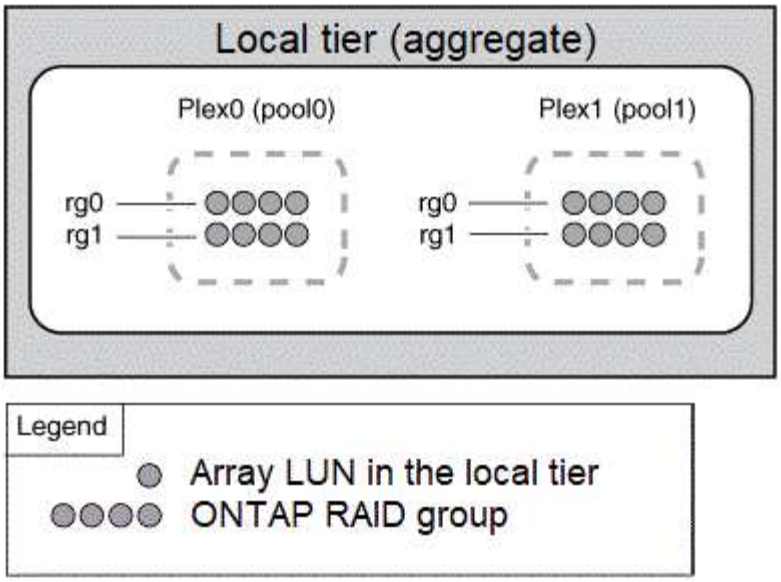
Essa configuração oferece proteção adicional contra a perda de dados se mais discos falharem do que o nível RAID do agregado protege contra ou se houver perda de conetividade, porque o Plex não afetado continua fornecendo dados enquanto você corrige a causa da falha. Depois que o Plex que teve um problema é corrigido, os dois plexos ressincronizam e restabelecem a relação do espelho.

Os discos e LUNs de array no sistema são divididos em dois pools: "'pool0'" e "'pool1". Plex0 obtém seu armazenamento de pool0GB e plex1GB recebe seu armazenamento de pool1GB.

O diagrama a seguir mostra um nível local composto por discos com a funcionalidade SyncMirror ativada e implementada. Um segundo Plex foi criado para o nível local, ""plex1"". Os dados em plex1 são uma cópia dos dados em plex0 e os grupos RAID também são idênticos. Os 32 discos sobressalentes são alocados para pool0 ou pool1 usando 16 discos para cada pool.



O diagrama a seguir mostra um nível local composto por LUNs de array com a funcionalidade SyncMirror ativada e implementada. Um segundo Plex foi criado para o nível local, ""plex1"". Plex1 é uma cópia do plex0 e os grupos RAID também são idênticos.



É recomendável manter pelo menos 20% de espaço livre para agregados espelhados para performance e disponibilidade ideais de storage. Embora a recomendação seja de 10% para agregados não espelhados, os 10% adicionais de espaço podem ser usados pelo sistema de arquivos para absorver alterações incrementais. Mudanças incrementais aumentam a utilização de espaço para agregados espelhados devido à arquitetura baseada em Snapshot copy-on-write da ONTAP. O não cumprimento destas práticas recomendadas pode ter um impactos negativo no desempenho.

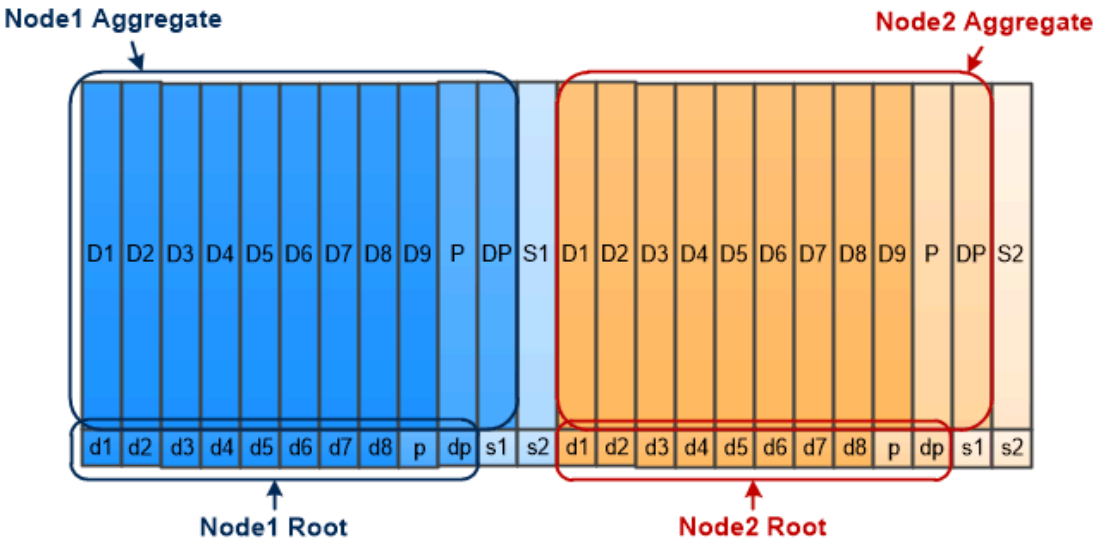
Particionamento de dados raiz

Cada nó deve ter um agregado de raiz para arquivos de configuração do sistema de storage. O agregado raiz tem o tipo RAID do agregado de dados.

O System Manager não suporta o particionamento root-data ou root-data-data-data.

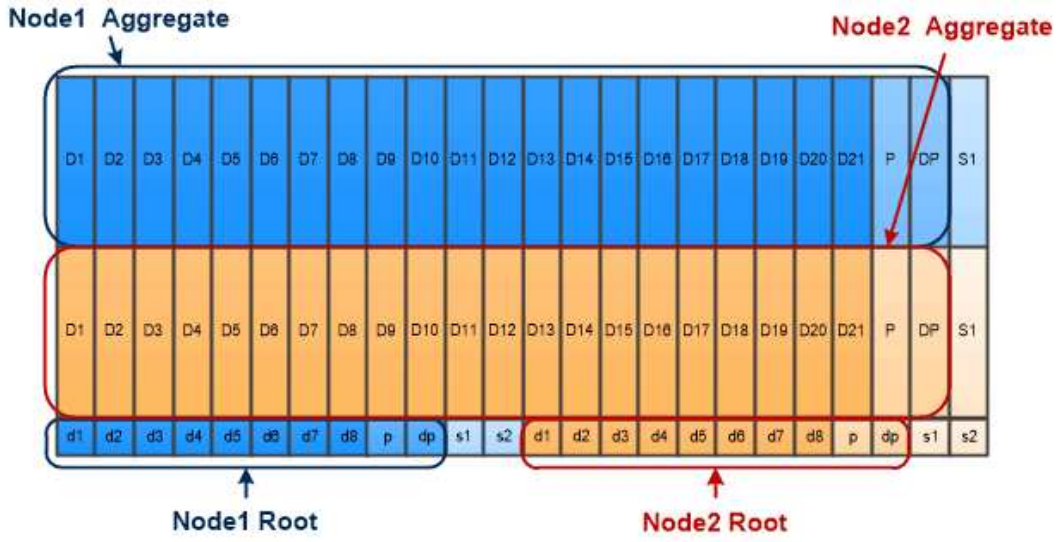
Um agregado de raiz do tipo RAID-DP normalmente consiste em um disco de dados e dois discos de paridade. Isso é um "imposto de paridade" significativo para pagar pelos arquivos do sistema de armazenamento, quando o sistema já está reservando dois discos como discos de paridade para cada grupo RAID no agregado.

Root-data partitioning reduz o imposto de paridade ao dividir o agregado de raiz entre partições de disco, reservando uma pequena partição em cada disco como partição raiz e uma grande partição para dados.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

Como a ilustração sugere, quanto mais discos forem usados para armazenar o agregado raiz, menor a partição raiz. Esse também é o caso de uma forma de particionamento de dados-raiz chamada *root-data-data-data partitioning*, que cria uma pequena partição como a partição raiz e duas partições maiores, igualmente dimensionadas para dados.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Ambos os tipos de particionamento de dados raiz fazem parte do recurso ONTAP *Advanced Drive Partitioning (ADP)*. Ambos são configurados de fábrica: Particionamento de dados raiz para sistemas FAS2xxx, FAS9000, FAS8200, FAS80xx e AFF de nível básico, particionamento de dados-raiz apenas para sistemas AFF.

Saiba mais "Advanced Drive Partitioning"sobre o .

Unidades particionadas e usadas para o agregado raiz

As unidades particionadas para uso no agregado raiz dependem da configuração do sistema.

Saber quantas unidades são usadas para o agregado raiz ajuda você a determinar quanto da capacidade das unidades é reservada para a partição raiz e quanto está disponível para uso em um agregado de dados.

A funcionalidade de particionamento de dados raiz é compatível com plataformas de nível básico, todas as plataformas Flash FAS e plataformas FAS com apenas SSDs anexados.

Para plataformas de nível básico, apenas as unidades internas são particionadas.

Para todas as plataformas Flash FAS e plataformas FAS com apenas SSDs conetados, todas as unidades conetadas ao controlador quando o sistema é inicializado são particionadas, até um limite de 24 TB por nó. As unidades adicionadas após a configuração do sistema não são particionadas.

Volumes, qtrees, arquivos e LUNs

O ONTAP serve dados para clientes e hosts de contentores lógicos chamados *FlexVol volumes.* porque esses volumes são apenas vagamente acoplados ao agregado que contém, eles oferecem maior flexibilidade no gerenciamento de dados do que os volumes tradicionais.

É possível atribuir vários volumes do FlexVol a um agregado, cada um dedicado a um aplicativo ou serviço diferente. Você pode expandir e contratar um FlexVol volume, mover um FlexVol volume e fazer cópias eficientes de um FlexVol volume. Você pode usar *qtrees* para particionar um FlexVol volume em unidades mais gerenciáveis e *cotas* para limitar o uso de recursos de volume.

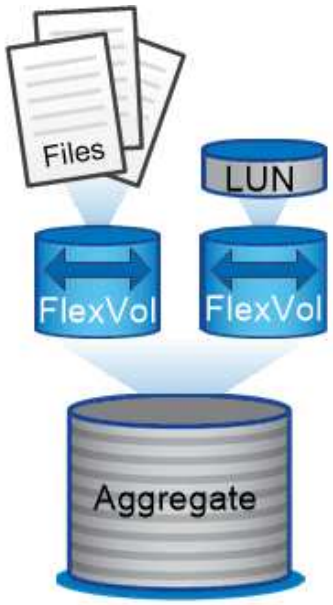
Os volumes contêm sistemas de arquivos em um ambiente nas e LUNs em um ambiente SAN. Um LUN (número de unidade lógica) é um identificador para um dispositivo chamado *unidade lógica* endereçado por um protocolo SAN.

LUNs são a unidade básica de armazenamento em uma configuração SAN. O host do Windows vê LUNs no seu sistema de armazenamento como discos virtuais. Migre LUNs para volumes diferentes sem interrupções, conforme necessário.

Além dos volumes de dados, há alguns volumes especiais que você precisa saber sobre:

- Um volume de raiz *node* (normalmente "'vol0") contém informações e logs de configuração do nó.
- Um volume raiz *SVM* serve como ponto de entrada para o namespace fornecido pelo SVM e contém informações de diretório de namespace.
- *Volumes do sistema* contêm metadados especiais, como logs de auditoria de serviço.

Você não pode usar esses volumes para armazenar dados.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

FlexGroup volumes

Em algumas empresas, um único namespace pode exigir petabytes de storage, excedendo até mesmo a capacidade de 100TB TB do FlexVol volume.

Um volume *FlexGroup* suporta até 400 bilhões de arquivos com 200 volumes de membros constituintes que trabalham de forma colaborativa para equilibrar dinamicamente a alocação de carga e espaço uniformemente entre todos os membros.

Não há sobrecarga necessária de manutenção ou gerenciamento com um volume FlexGroup. Basta criar o volume FlexGroup e compartilhá-lo com seus clientes nas. ONTAP faz o resto.

Virtualização de storage

Visão geral da virtualização de storage

Você usa *máquinas virtuais de armazenamento (SVMs)* para fornecer dados a clientes e hosts. Como uma máquina virtual em execução em um hipervisor, uma SVM é uma entidade lógica que abstrai recursos físicos. Os dados acessados pelo SVM não ficam vinculados a um local no storage. O acesso à rede ao SVM não está vinculado a uma porta física.

Os SVMs eram anteriormente chamados de "vserver". A interface de linha de comando ONTAP ainda usa o termo "vserver".

Um SVM serve dados para clientes e hosts de um ou mais volumes, por meio de uma ou mais interfaces lógicas de rede (LIFs)_. Os volumes podem ser atribuídos a qualquer agregado de dados no cluster. LIFs podem ser hospedados por qualquer porta física ou lógica. Os volumes e LIFs podem ser movidos sem interromper o serviço de dados, não importando se você está realizando atualizações de hardware,

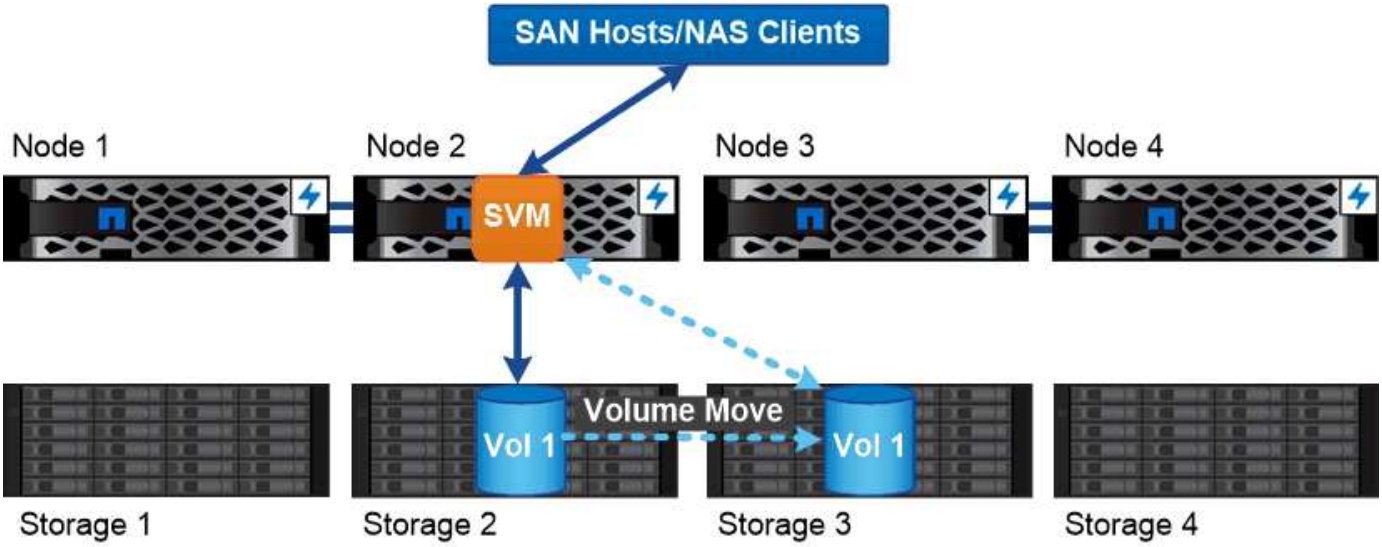
adicionando nós, equilibrando a performance ou otimizando a capacidade entre agregados.

O mesmo SVM pode ter um LIF para tráfego nas e um LIF para tráfego SAN. Os clientes e hosts precisam apenas do endereço do LIF (endereço IP para NFS, SMB ou iSCSI; WWPN para FC) para acessar o SVM. Os LIFs mantêm seus endereços à medida que se movem. As portas podem hospedar várias LIFs. Cada SVM tem sua própria segurança, administração e namespace.

Além de SVMs de dados, o ONTAP implanta SVMs especiais para administração:

- Um *admin SVM* é criado quando o cluster é configurado.
- Um *nó SVM* é criado quando um nó se junta a um cluster novo ou existente.
- Um *sistema SVM* é criado automaticamente para comunicações em nível de cluster em um IPspace.

Você não pode usar esses SVMs para fornecer dados. Há também LIFs especiais para tráfego dentro e entre clusters e para gerenciamento de clusters e nós.



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

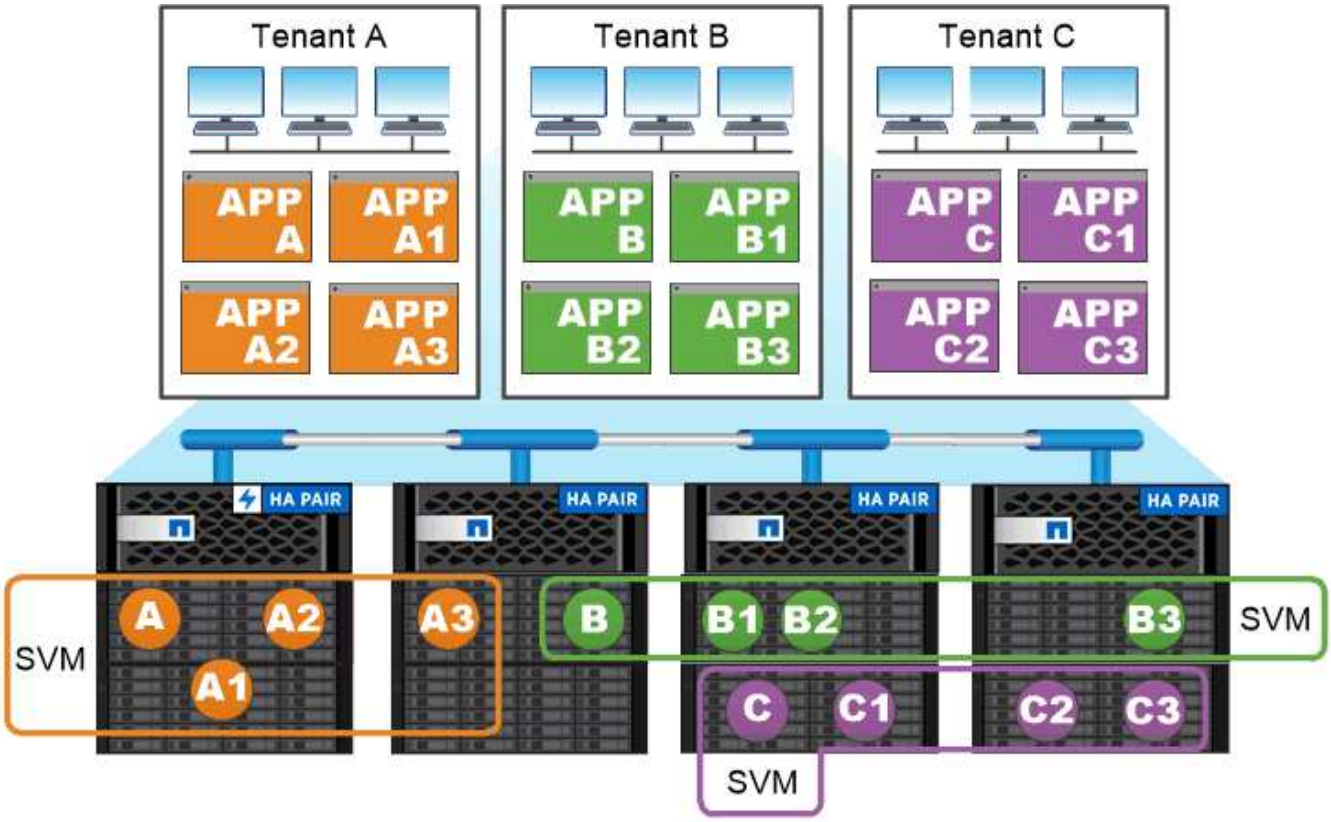
Por que ONTAP é como middleware

Os objetos lógicos que o ONTAP usa para tarefas de gerenciamento de armazenamento atendem aos objetivos familiares de um pacote de middleware bem projetado: Proteger o administrador de detalhes de implementação de baixo nível e isolar a configuração de alterações nas caraterísticas físicas, como nós e portas. A ideia básica é que o administrador deve ser capaz de mover volumes e LIFs facilmente, reconfigurando alguns campos em vez de toda a infraestrutura de armazenamento.

Casos de uso da SVM

Os fornecedores de serviços usam SVMs em acordos seguros de alocação a vários clientes para isolar os dados de cada locatário, fornecer a cada locatário sua própria autenticação e administração e simplificar o chargeback. Você pode atribuir vários LIFs ao mesmo SVM para atender a diferentes necessidades do cliente. Além disso, você pode usar a QoS para proteger contra cargas de trabalho de locatários "bullying" as cargas de trabalho de outros locatários.

Os administradores usam SVMs para fins semelhantes na empresa. Talvez você queira segregar dados de diferentes departamentos ou manter os volumes de storage acessados por hosts em um SVM e volumes de compartilhamento de usuários em outro. Alguns administradores colocam LUNs iSCSI/FC e armazenamentos de dados NFS em um SVM e compartilhamentos SMB em outro.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

Administração de clusters e SVM

Um *administrador de cluster* acessa o administrador SVM para o cluster. O administrador SVM e um administrador de cluster com o nome reservado `admin` são criados automaticamente quando o cluster é configurado.

Um administrador de cluster com a função padrão `admin` pode administrar todo o cluster e seus recursos. O administrador do cluster pode criar administradores de cluster adicionais com funções diferentes, conforme necessário.

Um *administrador do SVM* acessa um data SVM. O administrador do cluster cria SVMs de dados e administradores de SVM conforme necessário.

Por padrão, os administradores do SVM recebem `vsadmin` a função. O administrador do cluster pode atribuir funções diferentes aos administradores do SVM, conforme necessário.

Controle de Acesso baseado em função (RBAC)

A *função* atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Namespaces e pontos de junção

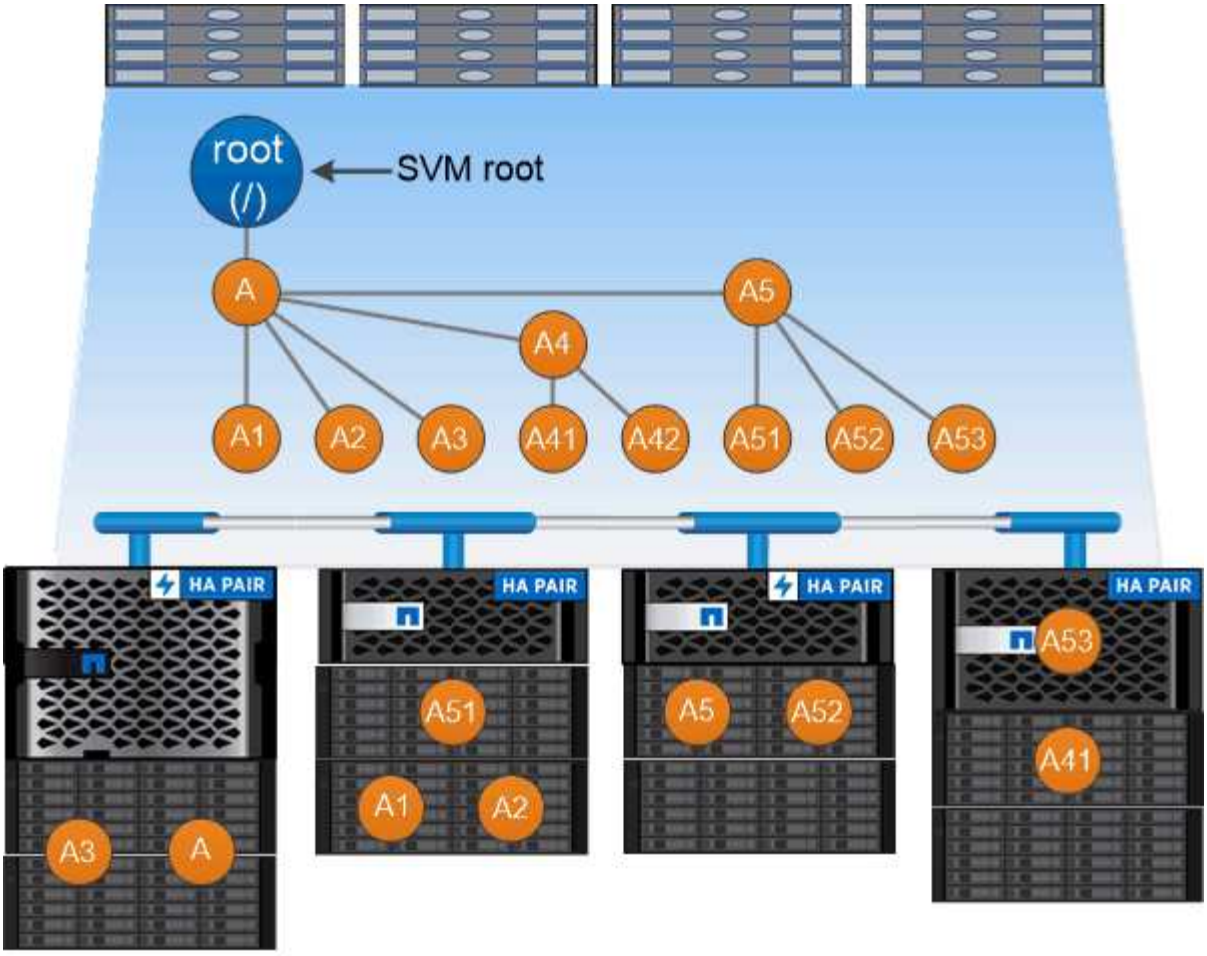
Um nas *namespace* é um agrupamento lógico de volumes Unidos em *pontos de junção* para criar uma única hierarquia de sistema de arquivos. Um cliente com permissões suficientes pode acessar arquivos no namespace sem especificar a localização dos arquivos no armazenamento. Os volumes Junctioned podem residir em qualquer lugar do cluster.

Em vez de montar cada volume contendo um arquivo de interesse, os clientes nas montam um NFS *export* ou acessam um SMB *share.* a exportação ou compartilhamento representa todo o namespace ou um local intermediário dentro do namespace. O cliente acessa apenas os volumes montados abaixo do seu ponto de acesso.

Você pode adicionar volumes ao namespace conforme necessário. Você pode criar pontos de junção diretamente abaixo de uma junção de volume pai ou em um diretório dentro de um volume. Um caminho para uma junção de volume para um volume chamado "'vol3" pode ser `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou mesmo `/dir1/dir2/vol3`. O caminho é chamado de *caminho de junção.*

Cada SVM tem um namespace único. O volume raiz da SVM é o ponto de entrada para a hierarquia de namespace.

Para garantir que os dados permaneçam disponíveis no caso de uma interrupção do nó ou failover, você deve criar uma cópia de *load-sharing mirror* para o volume raiz da SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Failover de caminho

Visão geral do failover de caminho

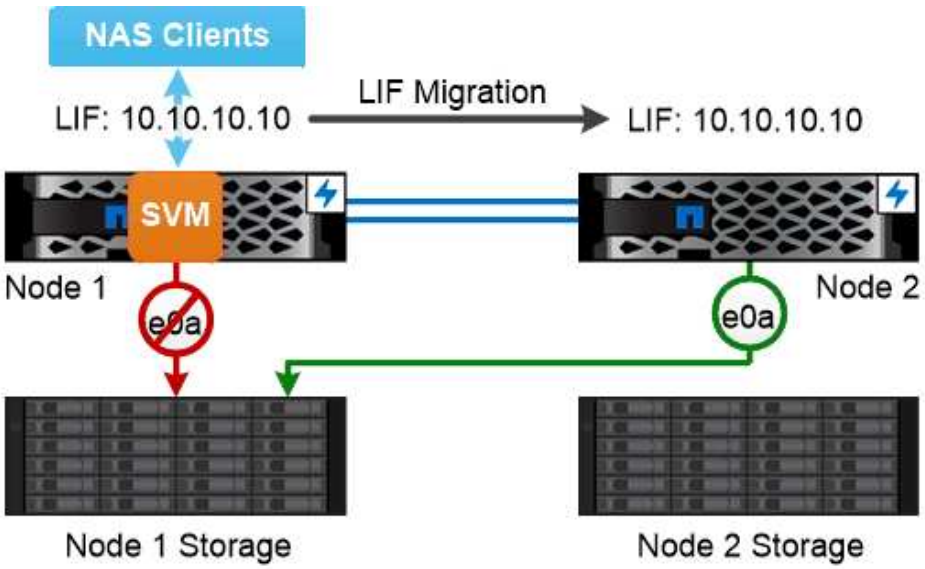
Há diferenças importantes em como o ONTAP gerencia o failover de caminho em topologias nas e SAN. Um LIF nas migra automaticamente para uma porta de rede diferente após uma falha de link. Um SAN LIF não migra (a menos que você o mova manualmente após a falha). Em vez disso, a tecnologia multipathing no host desvia o tráfego para um LIF diferente - no mesmo SVM, mas acessando uma porta de rede diferente.

Failover de caminho nas

Um LIF nas migra automaticamente para uma porta de rede sobrevivente após uma falha de link em sua porta atual. A porta para a qual o LIF migra deve ser um membro do grupo *failover* para o LIF. A política de grupo *failover* restringe os destinos de failover para um LIF de dados para portas no nó que possui os dados e seu parceiro de HA.

Para conveniência administrativa, o ONTAP cria um grupo de failover para cada domínio *broadcast* na arquitetura de rede. Os domínios de broadcast agrupam portas que pertencem à mesma rede de camada 2. Se você estiver usando VLANs, por exemplo, para segregar o tráfego por departamento (Engenharia, Marketing, Finanças e assim por diante), cada VLAN define um domínio de broadcast separado. O grupo de failover associado ao domínio de broadcast é atualizado automaticamente sempre que você adicionar ou remover uma porta de domínio de broadcast.

É quase sempre uma boa ideia usar um domínio de broadcast para definir um grupo de failover para garantir que o grupo de failover permaneça atual. Ocasionalmente, no entanto, você pode querer definir um grupo de failover que não esteja associado a um domínio de broadcast. Por exemplo, você pode querer que LIFs fail over apenas para portas em um subconjunto das portas definidas no domínio de broadcast.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

sub-redes

Uma *sub-rede* reserva um bloco de endereços IP em um domínio de broadcast. Esses endereços pertencem à mesma rede de camada 3 e são alocados às portas no domínio de broadcast quando você cria um LIF. Geralmente é mais fácil e menos propenso a erros especificar um nome de sub-rede quando você define um endereço LIF do que especificar um endereço IP e uma máscara de rede.

Failover de caminho SAN

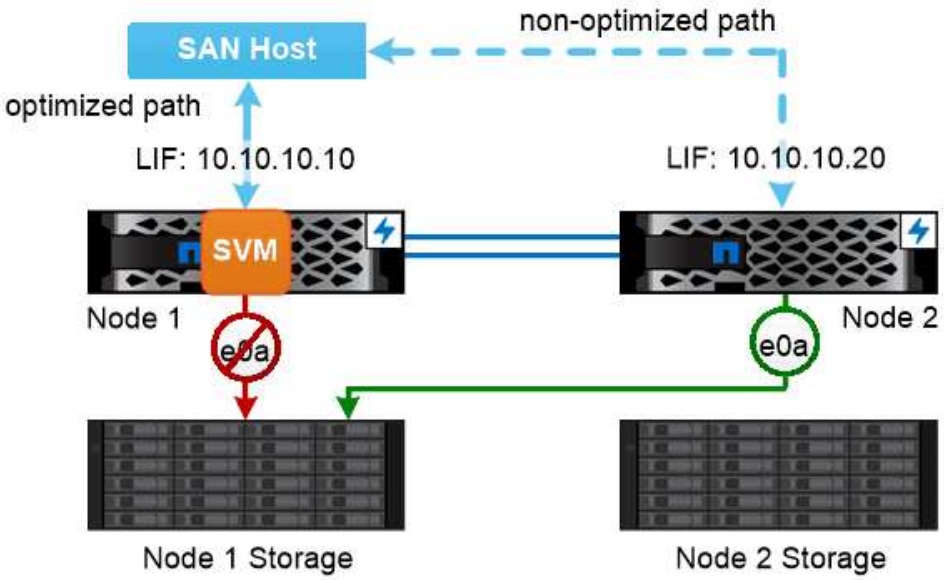
Um host SAN usa ALUA (Asymmetric Logical Unit Access) e MPIO (multipath I/o) para redirecionar o tráfego para um LIF sobrevivente após uma falha de link. Caminhos

predefinidos determinam as possíveis rotas para o LUN servido pelo SVM.

Em um ambiente SAN, os hosts são considerados como *iniciadores* de solicitações para LUN *destinos.* o MPIO habilita vários caminhos de iniciadores para destinos. ALUA identifica os caminhos mais diretos, chamados *caminhos otimizados.*

Normalmente, você configura vários caminhos otimizados para LIFs no nó proprietário do LUN e vários caminhos não otimizados para LIFs em seu parceiro de HA. Se uma porta falhar no nó proprietário, o host roteia o tráfego para as portas sobreviventes. Se todas as portas falharem, o host roteia o tráfego pelos caminhos não otimizados.

Por padrão, o ONTAP Selective LUN Map (SLM) limita o número de caminhos do host para um LUN. Um LUN recém-criado só pode ser acessado por meio de caminhos para o nó que possui o LUN ou seu parceiro de HA. Você também pode limitar o acesso a um LUN configurando LIFs em um *conjunto de portas* para o iniciador.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

movendo volumes em ambientes SAN

Por padrão, o ONTAP *Selective LUN Map (SLM)* limita o número de caminhos para um LUN de um host SAN. Um LUN recém-criado só pode ser acessado por meio de caminhos para o nó que possui o LUN ou seu parceiro de HA, os *nodos de relatórios* para o LUN.

Isso significa que, quando você move um volume para um nó em outro par de HA, você precisa adicionar nós de geração de relatórios para o par de HA de destino ao mapeamento de LUN. Em seguida, você pode especificar os novos caminhos na configuração do MPIO. Depois que a movimentação de volume estiver concluída, você poderá excluir os nós de relatório do par de HA de origem do mapeamento.

Balanceamento de carga

O desempenho de workloads começa a ser afetado pela latência quando a quantidade de trabalho em um nó excede os recursos disponíveis. Você pode gerenciar um nó

sobrecarregado aumentando os recursos disponíveis (atualizando discos ou CPU) ou reduzindo a carga (movendo volumes ou LUNs para nós diferentes, conforme necessário).

Você também pode usar a qualidade do serviço (QoS) do ONTAP para garantir que a performance de workloads essenciais não seja degradada pelos workloads da concorrência:

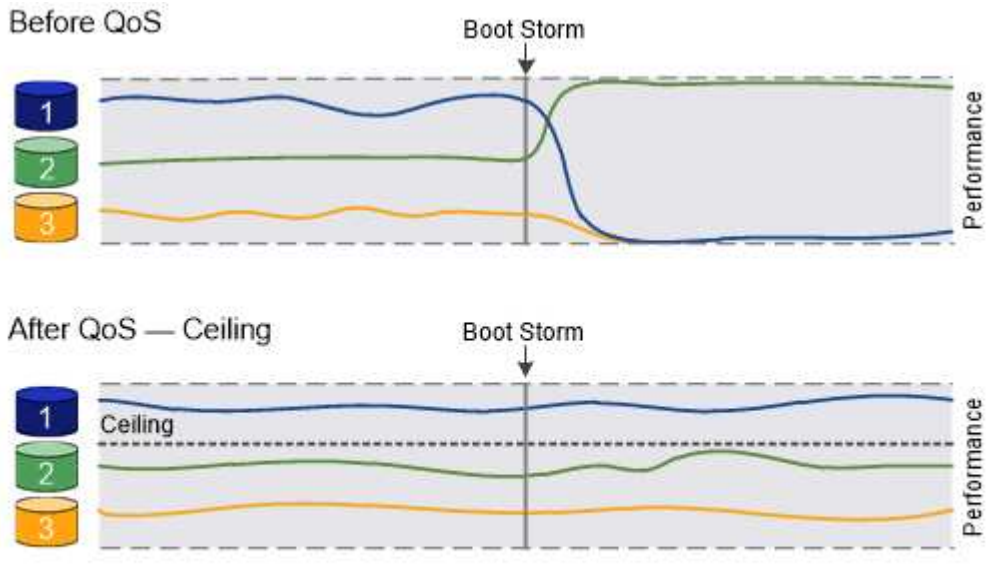
- Você pode definir uma taxa de transferência de QoS *ceiling* em um workload da concorrência para limitar seu impacto nos recursos do sistema (QoS Max).
- Você pode definir uma taxa de transferência de QoS *floor* para um workload crítico, garantindo que ele atenda aos destinos mínimos de taxa de transferência, independentemente da demanda por workloads da concorrência (QoS min).
- Você pode definir um limite e um espaço de QoS para o mesmo workload.

Limites máximos de taxa de transferência

Um limite máximo de taxa de transferência limita a taxa de transferência de uma carga de trabalho a um número máximo de IOPS ou MB/s. Na figura abaixo, o limite máximo de produtividade para a carga de trabalho 2 garante que não seja "bully" cargas de trabalho 1 e 3.

Um *grupo de políticas* define o limite máximo de taxa de transferência para uma ou mais cargas de trabalho. Um workload representa as operações de e/S de um *objeto de storage:* um volume, arquivo ou LUN ou todos os volumes, arquivos ou LUNs em uma SVM. Você pode especificar o limite máximo ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.

A taxa de transferência para cargas de trabalho pode exceder o limite máximo especificado em até 10%, especialmente se uma carga de trabalho sofrer mudanças rápidas na taxa de transferência. O teto pode ser excedido em até 50% para lidar com explosões.



The throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.

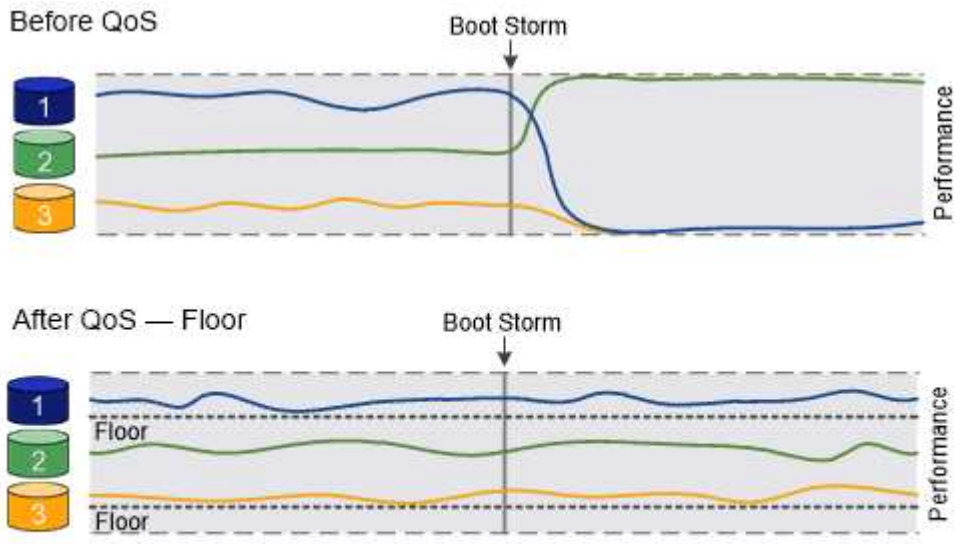
Andares com taxa de transferência

Um piso de taxa de transferência garante que a taxa de transferência para um workload não fique abaixo de um número mínimo de IOPS. Na figura abaixo, os andares de taxa de transferência para o workload 1 e o workload 3 garantem que eles atendam aos destinos mínimos de taxa de transferência, independentemente da demanda por workload 2.

Como os exemplos sugerem, um teto de throughput limita a taxa de transferência diretamente. Um piso de taxa de transferência mantém a taxa de transferência indiretamente, dando prioridade às cargas de trabalho para as quais o piso foi definido.

Uma carga de trabalho representa as operações de e/S de um volume, LUN ou, a partir de ONTAP 9.3, arquivo. Um grupo de políticas que define um piso de taxa de transferência não pode ser aplicado a um SVM. Você pode especificar o piso ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.

A taxa de transferência para uma carga de trabalho pode ficar abaixo do nível especificado se houver capacidade de desempenho (espaço livre) insuficiente no nó ou no agregado, ou durante operações críticas como `volume move trigger-cutover`o . Mesmo quando a capacidade suficiente está disponível e as operações críticas não estão ocorrendo, a taxa de transferência para uma carga de trabalho pode cair abaixo do piso especificado em até 5%.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

QoS adaptável

Normalmente, o valor do grupo de políticas que você atribui a um objeto de storage é fixo. Você precisa alterar o valor manualmente quando o tamanho do objeto de armazenamento muda. Um aumento na quantidade de espaço usado em um volume, por exemplo, geralmente requer um aumento correspondente no limite de produtividade especificado para o volume.

O *Adaptive QoS* dimensiona automaticamente o valor do grupo de políticas para o tamanho do workload, mantendo a taxa de IOPS para TBs|GBs conforme o tamanho do workload muda. Essa é uma vantagem significativa quando você gerencia centenas ou milhares de cargas de trabalho em uma implantação grande.

Normalmente, você usa QoS adaptável para ajustar limites máximos de taxa de transferência, mas também pode usá-la para gerenciar andares de taxa de transferência (quando o tamanho do workload aumenta). O tamanho do workload é expresso como o espaço alocado para o objeto de storage ou o espaço usado pelo objeto de storage.

O espaço usado está disponível para pisos de throughput no ONTAP 9.5 e posterior. Não é suportado para pisos de rendimento no ONTAP 9 .4 e anteriores.

A partir do ONTAP 9.13,1, você pode usar QoS adaptável para definir pisos e tetos de taxa de transferência no nível da SVM.

- Uma política *allocated space* mantém a relação IOPS/TB|GB de acordo com o tamanho nominal do objeto de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB terá um limite máximo de taxa de transferência de 15.000 IOPS enquanto o volume permanecer nesse tamanho. Se o volume for redimensionado para 300 GB, a QoS adaptável ajusta o limite da taxa de transferência para 30.000 IOPS.
- Uma política *used space* (o padrão) mantém a taxa IOPS/TB|GB de acordo com a quantidade de dados reais armazenados antes da eficiência de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB que tenha 100 GB de dados armazenados teria um limite máximo de taxa de transferência de 10.000 IOPS. À medida que a quantidade de espaço usado muda, a QoS adaptável ajusta o teto de taxa de transferência de acordo com a taxa.

Replicação

Cópias Snapshot

Tradicionalmente, as tecnologias de replicação da ONTAP atenderam à necessidade de recuperação de desastres (DR) e arquivamento de dados. Com o advento dos serviços de nuvem, a replicação do ONTAP foi adaptada à transferência de dados entre pontos de extremidade no NetApp Data Fabric. A base para todos esses usos é a tecnologia ONTAP Snapshot.

Uma *cópia Snapshot* é uma imagem pontual e somente leitura de um volume. Depois que uma cópia Snapshot é criada, o sistema de arquivos ativo e a cópia Snapshot apontam para os mesmos blocos de disco; portanto, a cópia Snapshot não usa espaço extra em disco. Com o tempo, a imagem consome espaço de armazenamento mínimo e incorre em uma sobrecarga de desempenho insignificante, pois Registra apenas alterações nos arquivos desde que a última cópia Snapshot foi feita.

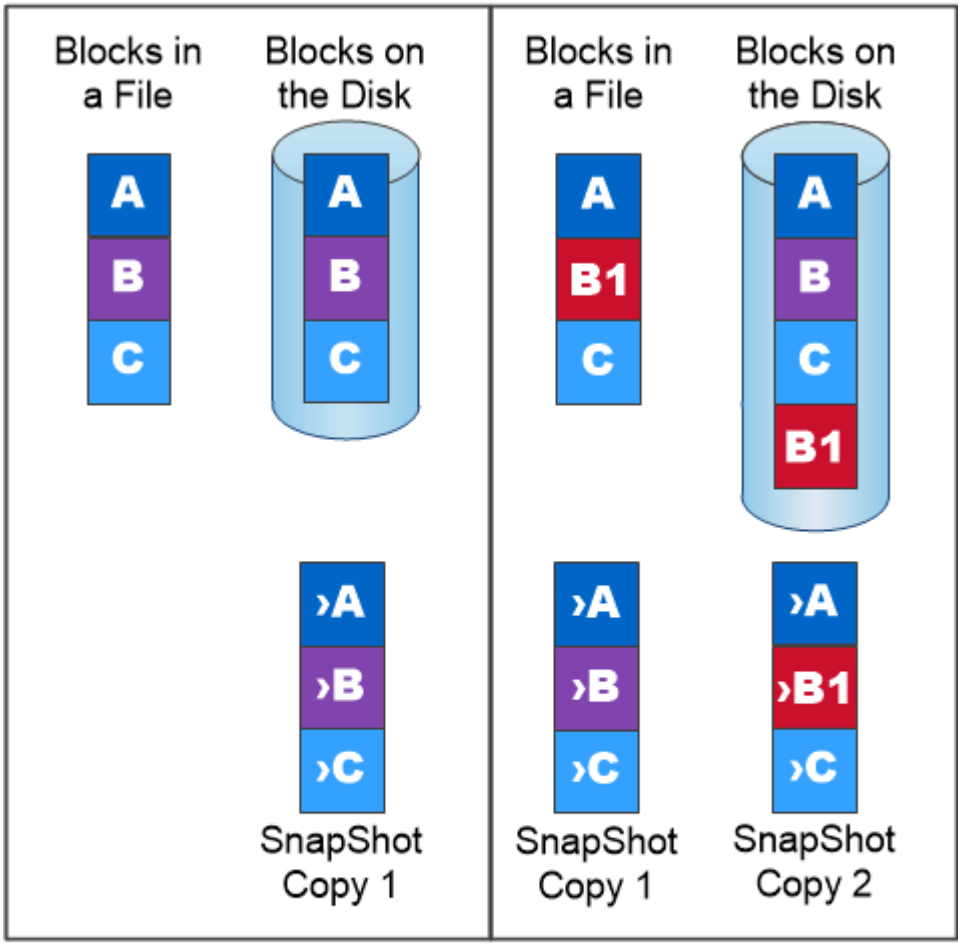
As cópias snapshot devem sua eficiência à tecnologia de virtualização de storage central da ONTAP, seu *Write Anywhere File Layout (WAFL).* como um banco de dados, o WAFL usa metadados para apontar para blocos de dados reais no disco. Mas, ao contrário de um banco de dados, o WAFL não substitui os blocos existentes. Ele grava dados atualizados em um novo bloco e altera os metadados.

As cópias snapshot são eficientes porque, em vez disso, copiar blocos de dados, o ONTAP faz referência aos metadados ao criar uma cópia Snapshot. Isso elimina tanto o "tempo de busca" que outros sistemas incorrem em localizar os blocos a copiar e o custo de fazer a cópia em si.

Você pode usar uma cópia Snapshot para recuperar arquivos individuais ou LUNs ou restaurar todo o conteúdo de um volume. O ONTAP compara as informações do ponteiro na cópia Snapshot com os dados no disco para reconstruir o objeto em falta ou danificado, sem tempo de inatividade ou um custo significativo de desempenho.

Uma política *Snapshot* define como o sistema cria cópias Snapshot de volumes. A política especifica quando criar as cópias Snapshot, quantas cópias devem ser mantidas, como nomeá-las e como rotulá-las para

replicação. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes, nomeá-las "diárias" (anexadas com um carimbo de data/hora) e rotulá-las "diárias" para replicação.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Recuperação de desastres da SnapMirror e transferência de dados

SnapMirror é uma tecnologia de recuperação de desastres, projetada para failover de armazenamento primário para armazenamento secundário em um local geograficamente remoto. Como o nome indica, o SnapMirror cria uma réplica, ou *mirror,* dos seus dados de trabalho em armazenamento secundário a partir do qual você pode continuar a servir dados em caso de uma catástrofe no local principal.

Os dados são espelhados no nível do volume. A relação entre o volume de origem no armazenamento primário e o volume de destino no armazenamento secundário é chamada de *relação de proteção de dados.* os clusters nos quais os volumes residem e os SVMs que servem dados dos volumes devem ser *peered.* Uma relação de mesmo nível permite que clusters e SVMs troquem dados com segurança.

Você também pode criar uma relação de proteção de dados entre SVMs. Nesse tipo de relacionamento, toda ou parte da configuração do SVM, de exportações de NFS e compartilhamentos de SMB para RBAC, são replicados, bem como os dados nos volumes de sua propriedade.

A partir do ONTAP 9.10,1, você pode criar relacionamentos de proteção de dados entre buckets do S3 usando o SnapMirror S3. Buckets de destino podem estar em sistemas ONTAP locais ou remotos, ou em sistemas que não sejam da ONTAP, como StorageGRID e AWS.

Na primeira vez que você invocar o SnapMirror, ele executa uma *transferência de linha de base* do volume de origem para o volume de destino. A transferência de linha de base normalmente envolve as seguintes etapas:

- Faça uma cópia Snapshot do volume de origem.
- Transfira a cópia Snapshot e todos os blocos de dados que ela faz referência ao volume de destino.
- Transfira as cópias Snapshot restantes e menos recentes no volume de origem para o volume de destino para o caso de o espelhamento "ativo" estar corrompido.

Quando a transferência de linha de base estiver concluída, o SnapMirror transferirá apenas novas cópias Snapshot para o espelhamento. As atualizações são assíncronas, seguindo a programação configurada. A retenção espelha a política do Snapshot na origem. Você pode ativar o volume de destino com interrupção mínima em caso de desastre no local principal e reativar o volume de origem quando o serviço é restaurado.

Como o SnapMirror transfere apenas cópias Snapshot após a criação da linha de base, a replicação é rápida e sem interrupções. Como o caso de uso de failover indica, as controladoras no sistema secundário devem ser equivalentes ou quase equivalentes às controladoras no sistema primário para atender dados com eficiência do storage espelhado.

A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

usando SnapMirror para transferência de dados

Você também pode usar o SnapMirror para replicar dados entre pontos de extremidade no NetApp Data Fabric. Você pode escolher entre replicação única ou replicação recorrente ao criar a política do SnapMirror.

Backups da nuvem do SnapMirror para storage de objetos

O *SnapMirror Cloud* é uma tecnologia de backup e recuperação projetada para usuários do ONTAP que desejam transferir seus fluxos de trabalho de proteção de dados para a nuvem. As organizações que se afastam de arquiteturas herdadas de backup para fita podem usar o storage de objetos como um repositório alternativo para retenção e arquivamento de dados a longo prazo. A nuvem da SnapMirror fornece replicação de storage ONTAP a objeto como parte de uma estratégia incremental de backup para sempre.

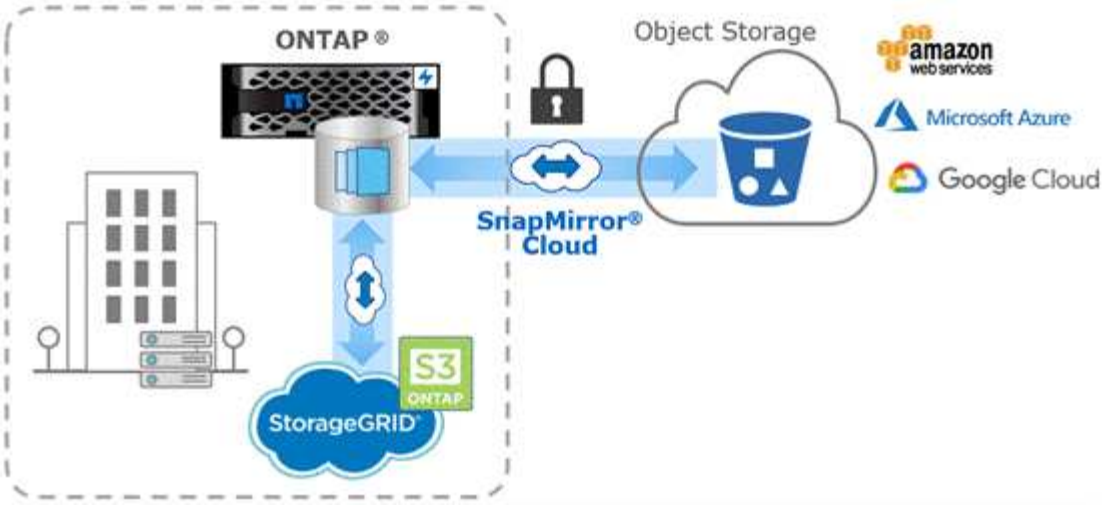
O SnapMirror Cloud foi apresentado no ONTAP 9.8 como uma extensão para a família de tecnologias de replicação do SnapMirror. Embora o SnapMirror seja frequentemente usado para backups de ONTAP para ONTAP, a nuvem do SnapMirror usa o mesmo mecanismo de replicação para transferir cópias Snapshot para ONTAP para backups de storage de objetos em conformidade com S3.

Destinado a casos de uso de backup, o SnapMirror Cloud é compatível com fluxos de trabalho de arquivos e retenção de longo prazo. Assim como no SnapMirror, o backup inicial na nuvem do SnapMirror realiza uma transferência de linha de base de um volume. Para backups subsequentes, o SnapMirror Cloud gera uma cópia snapshot do volume de origem e transfere a cópia snapshot somente com os blocos de dados alterados para um destino de storage de objetos.

As relações de nuvem do SnapMirror podem ser configuradas entre sistemas ONTAP e determinados destinos de storage de objetos no local e na nuvem pública, incluindo Amazon S3, Google Cloud Storage e storage de Blobs do Microsoft Azure. Destinos adicionais de storage de objetos no local incluem o StorageGRID e o ONTAP S3.

A replicação de nuvem do SnapMirror é um recurso licenciado da ONTAP e requer uma aplicação aprovada para orquestrar fluxos de trabalho de proteção de dados. Várias opções de orquestração estão disponíveis para o gerenciamento de backups de nuvem do SnapMirror:

- Vários parceiros de backup de 3rd partes que oferecem suporte para replicação na nuvem da SnapMirror. Os fornecedores participantes estão disponíveis no "NetApp blog".
- Backup e recuperação do BlueXP para uma solução nativa da NetApp para ambientes ONTAP
- APIs para desenvolver software personalizado para workflows de proteção de dados ou aproveitar ferramentas de automação



Arquivamento SnapVault

A licença do SnapMirror é usada para dar suporte às relações do SnapVault para backup e às relações do SnapMirror para recuperação de desastres. A partir do ONTAP 9.3, as licenças do SnapVault são obsoletas e as licenças do SnapMirror podem ser usadas para configurar relações de Vault, mirror e mirror-and-Vault. A replicação do SnapMirror é usada para replicação ONTAP para ONTAP de cópias Snapshot, compatível com casos de uso de backup e recuperação de desastres.

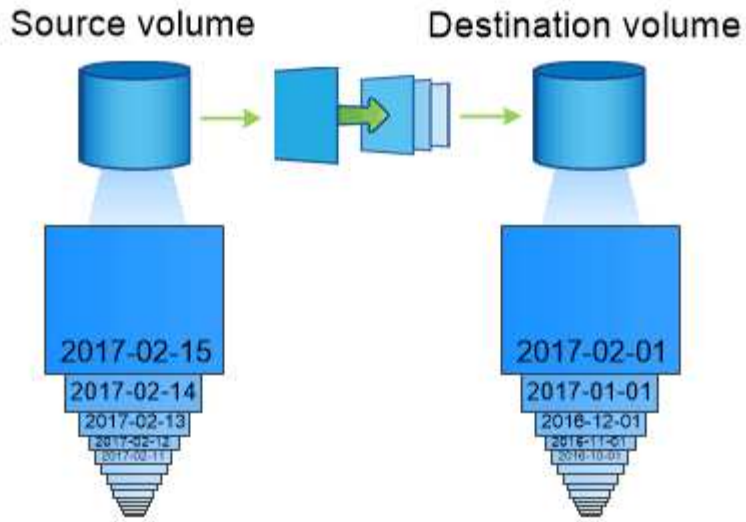
O *SnapVault* é uma tecnologia de arquivamento, projetada para replicação de cópias Snapshot de disco para disco para conformidade com padrões e outros fins relacionados à governança. Em contraste com uma relação do SnapMirror, em que o destino geralmente contém apenas as cópias Snapshot atualmente no volume de origem, um destino do SnapVault geralmente retém cópias Snapshot pontuais criadas por um período muito mais longo.

Por exemplo, você pode manter cópias Snapshot mensais de seus dados em um período de 20 anos, para cumprir com as regulamentações contábeis governamentais dos seus negócios. Como não há necessidade de fornecer dados do armazenamento do Vault, você pode usar discos mais lentos e menos caros no sistema de destino.

Tal como acontece com o SnapMirror, o SnapVault executa uma transferência de linha de base na primeira vez que você a invoca. Ele faz uma cópia Snapshot do volume de origem e, em seguida, transfere a cópia e os blocos de dados que ela faz referência ao volume de destino. Diferentemente do SnapMirror, o SnapVault não inclui cópias Snapshot mais antigas na linha de base.

As atualizações são assíncronas, seguindo a programação configurada. As regras definidas na política de relacionamento identificam quais novas cópias snapshot devem incluir nas atualizações e quantas cópias devem ser mantidas. Os rótulos definidos na política ("em quarto lugar", por exemplo) devem corresponder a um ou mais rótulos definidos na política de captura instantânea na origem. Caso contrário, a replicação falha.

SnapMirror e SnapVault compartilham a mesma infraestrutura de comando. Você especifica qual método deseja usar ao criar uma política. Ambos os métodos exigem clusters com peered e SVMs com peered.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Backup em nuvem e suporte para backups tradicionais

Além dos relacionamentos de proteção de dados do SnapMirror e do SnapVault, que eram disco a disco somente para o ONTAP 9.7 e anteriores, agora há várias soluções de backup que oferecem uma alternativa mais econômica para a retenção de dados a longo prazo.

Várias aplicações de proteção de dados de terceiros oferecem backup tradicional para dados gerenciados pela ONTAP. Veeam, Veritas e CommVault, entre outros, oferecem backup integrado para sistemas ONTAP.

A partir do ONTAP 9.8, a nuvem SnapMirror oferece replicação assíncrona de cópias Snapshot de instâncias do ONTAP para pontos de extremidade de storage de objetos. A replicação de nuvem do SnapMirror requer uma aplicação licenciada para orquestração e gerenciamento de workflows de proteção de dados. Os relacionamentos de nuvem da SnapMirror são compatíveis com sistemas ONTAP para selecionar destinos de storage de objetos no local e na nuvem pública, incluindo AWS S3, Google Cloud Storage Platform ou storage de Blobs do Microsoft Azure, o que fornece eficiência aprimorada com software de backup de fornecedor. Entre em Contato com seu representante da NetApp para obter uma lista de aplicativos certificados compatíveis e fornecedores de storage de objetos.

Se você estiver interessado em proteção de dados nativa da nuvem, o BlueXP pode ser usado para configurar relações SnapMirror ou SnapVault entre volumes no local e instâncias do Cloud Volumes ONTAP na nuvem pública.

O BlueXP também fornece backups de instâncias do Cloud Volumes ONTAP usando um modelo de software como serviço (SaaS). Os usuários podem fazer backup de suas instâncias do Cloud Volumes ONTAP em um storage de objetos em nuvem pública compatível com S3 e S3 usando o backup em nuvem no NetApp Central.

"Recursos de documentação do Cloud Volumes ONTAP e do BlueXP "

"Centro de nuvem da NetApp"

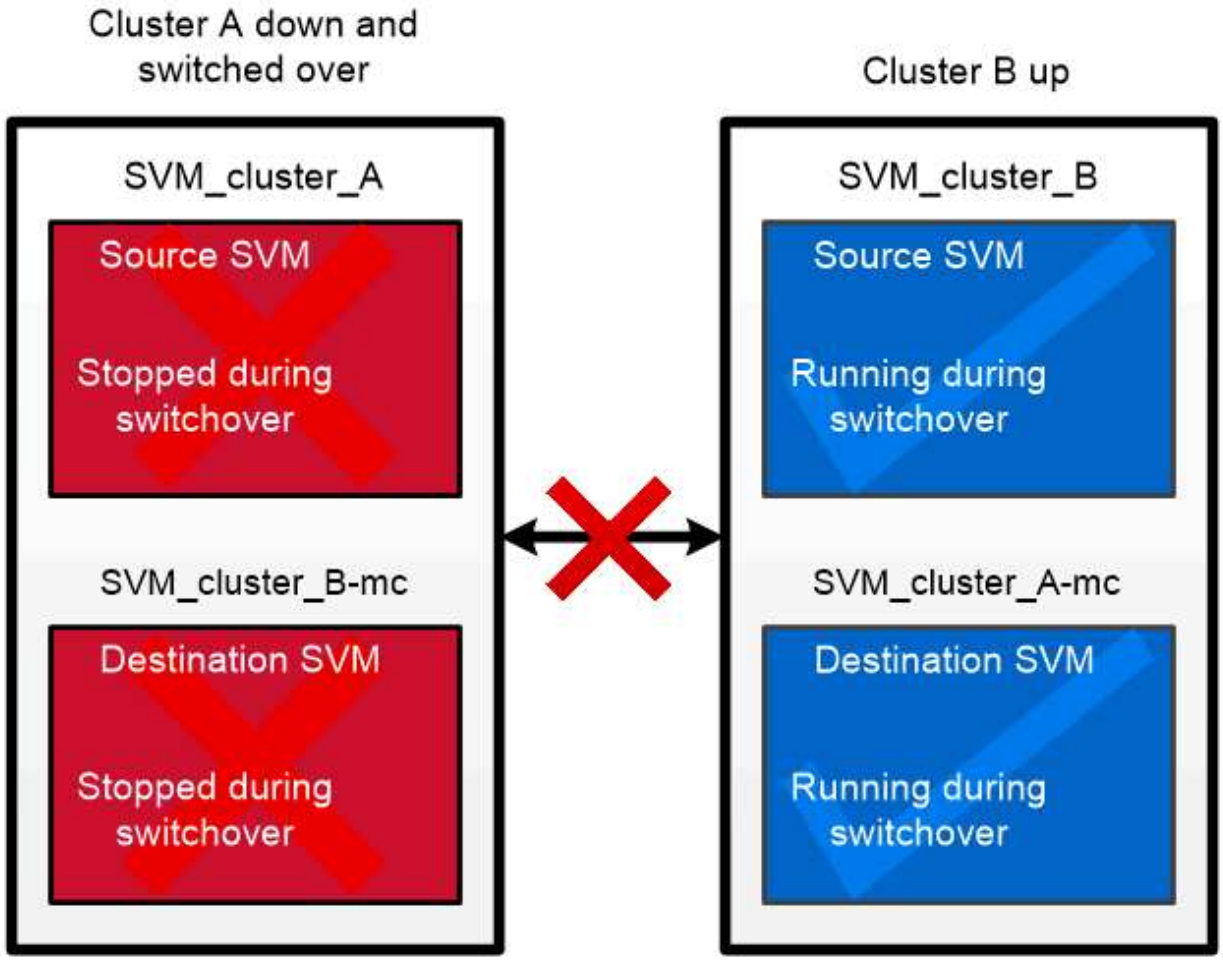
Disponibilidade contínua da MetroCluster

As configurações do MetroCluster protegem os dados com a implementação de dois clusters espelhados separados fisicamente. Cada cluster replica de forma síncrona os dados e a configuração da SVM do outro. Em caso de desastre em um local, o administrador pode ativar o SVM espelhado e começar a fornecer dados do local que sobreviveu.

- As configurações de *Fabric-Attached MetroCluster* e *MetroCluster IP* são compatíveis com clusters metropolitano.
- As configurações do *Stretch MetroCluster* suportam clusters em todo o campus.

Os clusters devem ser percorridos em ambos os casos.

O MetroCluster usa um recurso ONTAP chamado *SyncMirror* para espelhar sincronamente dados agregados para cada cluster em cópias ou *plexes* no armazenamento do outro cluster. Se ocorrer um switchover, o Plex remoto no cluster sobrevivente fica on-line e o SVM secundário começa a fornecer dados.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

Using SyncMirror em implementações não-MetroCluster você pode usar o SyncMirror em uma implementação não-MetroCluster para proteger contra perda de dados se mais discos falharem do que o tipo RAID protege contra, ou se houver perda de conetividade com discos do grupo RAID. O recurso está disponível somente para pares de HA.

Os dados agregados são espelhados em plexos armazenados em diferentes compartimentos de disco. Se uma das gavetas ficar indisponível, o Plex não afetado continuará fornecendo dados enquanto você corrigir a causa da falha.

Tenha em mente que um agregado espelhado usando o SyncMirror requer o dobro de storage que um agregado sem espelhamento. Cada Plex requer tantos discos quanto o Plex que ele espelha. Você precisaria de 2.880 GB de espaço em disco, por exemplo, para espelhar um agregado de 1.440 GB, 1.440 GB para cada Plex.

Com o SyncMirror, é recomendável manter pelo menos 20% de espaço livre para agregados espelhados para performance e disponibilidade ideais de storage. Embora a recomendação seja de 10% para agregados não espelhados, os 10% adicionais de espaço podem ser usados pelo sistema de arquivos para absorver alterações incrementais. Mudanças incrementais aumentam a utilização de espaço para agregados espelhados devido à arquitetura baseada em Snapshot copy-on-write da ONTAP. A não adesão a essas práticas recomendadas pode ter um impactos negativo no desempenho de ressincronização do SyncMirror, o que afeta indiretamente fluxos de trabalho operacionais, como NDU para implantações de nuvem não compartilhadas e switchback para implantações de MetroCluster.

O SyncMirror também está disponível para implementações de virtualização FlexArray.

Eficiência de storage

Visão geral da eficiência de storage da ONTAP

A eficiência de storage é a medida de como um sistema de storage utiliza o espaço disponível com a otimização dos recursos de storage, a minimização do desperdício de espaço e a redução do espaço físico dos dados gravados. Uma maior eficiência de storage permite armazenar a quantidade máxima de dados no menor espaço possível com o menor custo possível. Por exemplo, a utilização de tecnologias eficientes de storage que detetam e eliminam blocos de dados duplicados e blocos de dados preenchidos com zeros diminui a quantidade geral de storage físico de que você precisa e reduz o custo geral.

O ONTAP oferece uma ampla gama de tecnologias de eficiência de storage que reduzem a quantidade de hardware físico ou storage de nuvem consumida pelos dados, além de gerar melhorias significativas na performance do sistema, incluindo leituras mais rápidas de dados, cópias mais rápidas dos conjuntos de dados e provisionamento de VM mais rápido.

As tecnologias de eficiência de storage da ONTAP incluem:

- * Provisionamento thin*

  Thin Provisioning Permite alocar armazenamento em um volume ou LUN conforme necessário, em vez de reservá-lo com antecedência. Isso reduz a quantidade de storage físico de que você precisa, permitindo alocar em excesso seus volumes ou LUNs com base no uso potencial sem reservar espaço que não está sendo usado atualmente.

- **Desduplicação**

  Deduplicação reduz a quantidade de armazenamento físico necessária para um volume de três maneiras distintas.

  - **Deduplicação de bloco zero**

    A deduplicação de bloco zero deteta e elimina blocos de dados preenchidos com todos os zeros e apenas atualiza metadados. 100% do espaço normalmente usado por blocos zero é então salvo. A deduplicação de bloco zero é ativada por padrão em todos os volumes desduplicados.

  - **Deduplicação in-line**

    A deduplicação in-line deteta blocos de dados duplicados e os substitui por referências a um bloco compartilhado exclusivo antes que os dados sejam gravados no disco. A deduplicação in-line acelera o provisionamento de VM em 20% a 30%. Dependendo da sua versão do ONTAP e da sua plataforma, a deduplicação in-line está disponível no nível de volume ou agregado. Ele é habilitado por padrão em sistemas AFF e ASA. Você precisa habilitar manualmente a deduplicação in-line em sistemas FAS.

  - * Deduplicação em segundo plano*

    A deduplicação em segundo plano também deteta blocos de dados duplicados e os substitui por referências a um bloco compartilhado exclusivo. No entanto, aumenta ainda mais a eficiência de storage fazendo isso depois que os dados são gravados no disco. Você pode configurar a deduplicação em segundo plano para ser executada quando certos critérios são atendidos no sistema de storage. Por exemplo, você pode habilitar a deduplicação em segundo plano quando o volume atingir 10% de utilização. Você também pode acionar manualmente a deduplicação em segundo plano ou configurá-la para ser executada em um cronograma específico. Ele é habilitado por padrão em sistemas AFF e ASA. Você precisa habilitar manualmente a deduplicação em segundo plano em sistemas FAS.

  A deduplicação é compatível com volumes e volumes em um agregado. Leituras de dados deduplicados normalmente não implicam custos de desempenho.

- **Compressão**

  Compactação reduz a quantidade de storage físico necessária para um volume, combinando blocos de dados em grupos de compressão, cada um dos quais é armazenado como um único bloco. Quando uma solicitação de leitura ou substituição é recebida, apenas um pequeno grupo de blocos é lido, não o arquivo inteiro. Este processo otimiza o desempenho de leitura e substituição e permite uma maior escalabilidade no tamanho dos arquivos que estão sendo compatados.

  A compressão pode ser executada em linha ou no pós-processo. A compactação in-line proporciona economia imediata de espaço ao compactar dados na memória antes de serem gravados no disco. A compressão pós-processo primeiro grava os blocos no disco como descompactados e, em seguida, em um horário programado comprime os dados. Ele é habilitado por padrão em sistemas AFA. Você precisa ativar manualmente a compactação em todos os outros sistemas.

- **Compactação**

  A compactação reduz a quantidade de storage físico necessária para um volume, tomando blocos de dados armazenados em blocos de 4 KB, mas com menos de 4 KB de tamanho e combinando-os em um único bloco. A compactação ocorre enquanto os dados ainda estão na memória para que espaço desnecessário nunca seja consumido nos discos. Ele é habilitado por padrão em sistemas AFF e ASA. É necessário ativar manualmente a compactação em sistemas FAS.

- **Volumes, arquivos e LUNs do FlexClone**

  Tecnologia FlexClone Aproveita os metadados do Snapshot para criar cópias graváveis e pontuais de um volume, arquivo ou LUN. As cópias compartilham blocos de dados com os pais, não consumindo storage, exceto o necessário para os metadados até que as alterações sejam gravadas em uma cópia ou seu pai. Quando uma alteração é escrita, apenas o delta é armazenado.

  Onde as cópias tradicionais de conjuntos de dados podem levar minutos ou até horas para criar, a tecnologia FlexClone permite copiar até mesmo os maiores conjuntos de dados quase instantaneamente.

- * Eficiência de armazenamento sensível à temperatura*

  O ONTAP fornece "eficiência de storage sensível à temperatura" benefícios avaliando a frequência com que os dados do seu volume são acessados e mapeando essa frequência para o grau de compressão aplicado a esses dados. Para dados inativos acessados com pouca frequência, blocos de dados maiores são compatados. Para dados ativos acessados com frequência e substituídos com mais frequência, blocos de dados menores são compatados, tornando o processo mais eficiente.

  A eficiência de storage sensível à temperatura (TSSE), introduzida no ONTAP 9.8, é ativada automaticamente em volumes AFF recém-criados com provisionamento reduzido. Ele não está habilitado no "Plataformas AFF A70, AFF A90 e AFF A1K" que são introduzidos no ONTAP 9.15,1, que usam um processador de descarga de hardware.

- * CPU ou eficiência de armazenamento dedicado do processador de descarga*

  A partir do ONTAP 9.15,1, o ONTAP fornece "CPU ou eficiência de storage do processador de descarga dedicado" e dá compactação de dados nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90. Nos sistemas AFF A70, AFF A90 e AFF A1K, a eficiência de storage é ativada automaticamente e não requer configuração.

Você pode aproveitar essas tecnologias em suas operações diárias com o mínimo de esforço. Por exemplo, suponha que você precise fornecer 5.000 usuários com armazenamento para diretórios base, e você estima que o espaço máximo necessário para qualquer usuário é de 1 GB. Você pode reservar um agregado de 5 TB com antecedência para atender à necessidade total de storage potencial. No entanto, você também sabe que os requisitos de capacidade do diretório base variam muito em toda a sua organização. Em vez de reservar 5 TB de espaço total para sua organização, você pode criar um agregado de 2 TB. Em seguida, você pode usar thin Provisioning para atribuir nominalmente 1 GB de armazenamento a cada usuário, mas alocar o armazenamento apenas conforme necessário. Você pode monitorar ativamente o agregado ao longo do tempo e aumentar o tamanho físico real, conforme necessário.

Em outro exemplo, suponha que você esteja usando uma infraestrutura de desktop virtual (VDI) com uma grande quantidade de dados duplicados entre seus desktops virtuais. A deduplicação reduz o uso do storage eliminando automaticamente blocos duplicados de informações na VDI, substituindo-os por um ponteiro para o bloco original. Outras tecnologias de eficiência de storage da ONTAP, como a compactação, também podem ser executadas em segundo plano sem intervenção.

A tecnologia de particionamento de disco da ONTAP também oferece maior eficiência de storage. A tecnologia RAID DP protege contra falhas duplas de disco sem sacrificar o desempenho ou adicionar sobrecarga de espelhamento de disco. O particionamento avançado de SSD com ONTAP 9 aumenta a capacidade utilizável em quase 20%.

O NetApp fornece os mesmos recursos de eficiência de storage disponíveis no ONTAP local na nuvem. Ao migrar dados do ONTAP no local para a nuvem, a eficiência de storage existente é preservada. Por exemplo, suponha que você tenha um banco de dados SQL contendo dados essenciais aos negócios que deseja mover de um sistema local para a nuvem. Você pode usar a replicação de dados no BlueXP para migrar seus dados

e, como parte do processo de migração, ativar a política mais recente no local para cópias Snapshot na nuvem.

Thin Provisioning

A ONTAP oferece uma ampla variedade de tecnologias de eficiência de storage, além das cópias Snapshot. As principais tecnologias incluem thin Provisioning, deduplicação, compactação e volumes, arquivos e LUNs do FlexClone. Assim como as cópias Snapshot, todas são criadas no WAFL (Write Anywhere File Layout) do ONTAP.

Um volume ou LUN *thin-provisionado* é aquele para o qual o armazenamento não é reservado com antecedência. Em vez disso, o storage é alocado dinamicamente, conforme necessário. O espaço livre é liberado de volta ao sistema de armazenamento quando os dados no volume ou LUN são excluídos.

Suponha que sua organização precisa fornecer aos usuários do 5.000 o armazenamento para diretórios base. Você estima que os maiores diretórios base consumirão 1 GB de espaço.

Nesta situação, você pode comprar 5 TB de armazenamento físico. Para cada volume que armazena um diretório home, você reservaria espaço suficiente para satisfazer as necessidades dos maiores consumidores.

No entanto, como uma questão prática, você também sabe que os requisitos de capacidade do diretório base variam muito em toda a sua comunidade. Para cada grande usuário de armazenamento, há dez que consomem pouco ou nenhum espaço.

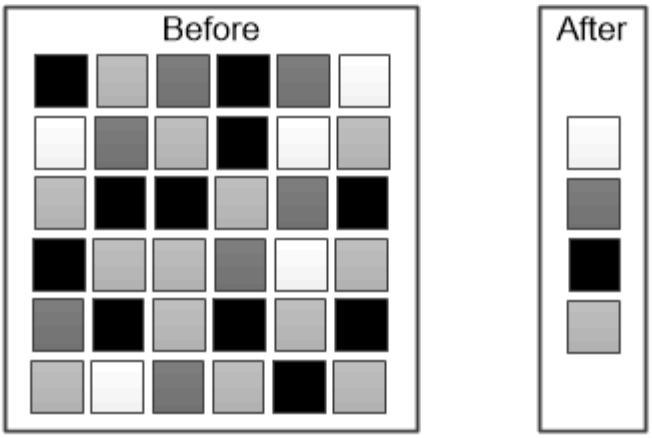
O thin Provisioning permite que você atenda às necessidades dos grandes consumidores de storage sem ter que comprar storage que você talvez nunca use. Como o espaço de armazenamento não é alocado até ser consumido, você pode "'comprometer'" um agregado de 2 TB, atribuindo nominalmente um tamanho de 1 GB a cada um dos 5.000 volumes que o agregado contém.

Contanto que você esteja correto que haja uma proporção de 10:1 de usuários leves para pesados, e contanto que você assuma um papel ativo no monitoramento de espaço livre no agregado, você pode ter certeza de que as gravações de volume não falharão devido à falta de espaço.

Deduplicação

Desduplicação reduz a quantidade de armazenamento físico necessária para um volume (ou todos os volumes em um agregado AFF) descartando blocos duplicados e substituindo-os por referências a um único bloco compartilhado. Leituras de dados deduplicados normalmente não implicam custos de desempenho. As gravações incorrem em uma cobrança insignificante, exceto em nós sobrecarregados.

À medida que os dados são gravados durante o uso normal, o WAFL usa um processo em lote para criar um catálogo de assinaturas de bloco._ depois que a deduplicação é iniciada, o ONTAP compara as assinaturas no catálogo para identificar blocos duplicados. Se existir uma correspondência, uma comparação byte-a-byte é feita para verificar se os blocos candidatos não foram alterados desde que o catálogo foi criado. Somente se todos os bytes corresponderem é o bloco duplicado descartado e seu espaço em disco recuperado.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

Compactação

Compression reduz a quantidade de armazenamento físico necessária para um volume combinando blocos de dados em *grupos de compressão,* cada um dos quais é armazenado como um único bloco. As leituras de dados compatados são mais rápidas do que nos métodos de compactação tradicionais porque o ONTAP descompacta apenas os grupos de compactação que contêm os dados solicitados, não um arquivo inteiro ou LUN.

Você pode executar a compressão inline ou pós-processo, separadamente ou em combinação:

- *Compactação in line* compacta os dados na memória antes de serem gravados no disco, reduzindo significativamente a quantidade de e/S de gravação em um volume, mas potencialmente degradando o desempenho de gravação. Operações intensivas em desempenho são adiadas até a próxima operação de compressão pós-processo, se houver.
- *Pós-process Compression* compacta os dados depois que eles são gravados no disco, no mesmo cronograma da deduplicação.

compactação de dados em linha pequenos arquivos ou e/S acolchoados com zeros são armazenados em um bloco de 4 KB, quer eles exijam ou não 4 KB de armazenamento físico. *Compactação de dados em linha* combina blocos de dados que normalmente consumiriam vários blocos de 4 KB em um único bloco de 4 KB no disco. A compactação ocorre enquanto os dados ainda estão na memória, por isso é mais adequada para controladoras mais rápidas.

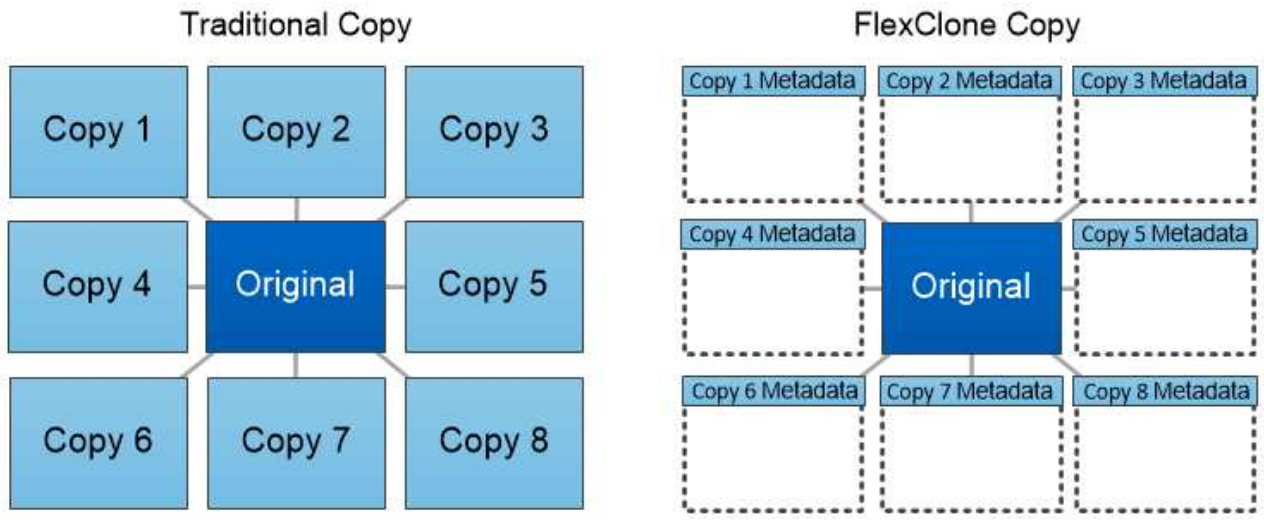
Volumes, arquivos e LUNs do FlexClone

A tecnologia *FlexClone* faz referência aos metadados do Snapshot para criar cópias graváveis e pontuais de um volume. As cópias compartilham blocos de dados com os pais, não consumindo storage, exceto o necessário para os metadados até que as alterações sejam gravadas na cópia. Os arquivos FlexClone e os LUNs FlexClone usam tecnologia idêntica, exceto que uma cópia Snapshot de backup não é necessária.

Onde as cópias tradicionais podem levar minutos ou até horas para criar, o software FlexClone permite copiar

até mesmo os maiores conjuntos de dados quase instantaneamente. Isso o torna ideal para situações em que você precisa de várias cópias de conjuntos de dados idênticos (uma implantação de desktop virtual, por exemplo) ou cópias temporárias de um conjunto de dados (testando uma aplicação em um conjunto de dados de produção).

Você pode clonar um volume FlexClone existente, clonar um volume contendo clones de LUN ou clonar dados espelhados e Vault. Você pode *dividir* um volume FlexClone de seu pai, caso em que a cópia é alocada seu próprio armazenamento.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

Medições de capacidade no System Manager

A capacidade do sistema pode ser medida como espaço físico ou espaço lógico. A partir do ONTAP 9.7, o Gerenciador de sistemas fornece medições de capacidade física e lógica.

As diferenças entre as duas medições são explicadas nas seguintes descrições:

- **Capacidade física**: O espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume ou nível local. O valor da capacidade física usada geralmente é menor do que o valor da capacidade lógica usada devido à redução de dados de recursos de eficiência de storage (como deduplicação e compactação).
- **Capacidade lógica**: O espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume ou nível local. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados da deduplicação ou compressão. O valor do espaço lógico usado é derivado da quantidade de espaço físico usado, além da economia com recursos de eficiência de storage (como deduplicação e compactação) configurados. Essa medição geralmente parece maior do que a capacidade física usada porque inclui cópias Snapshot, clones e outros componentes, e não reflete a compactação de dados e outras reduções no espaço físico. Assim, a capacidade lógica total poderia ser maior do que o espaço provisionado.

No System Manager, as representações de capacidade não são responsáveis pelas capacidades da camada de storage raiz (agregado).

Medições da capacidade utilizada

As medições da capacidade utilizada são apresentadas de forma diferente, dependendo da versão do System Manager que estiver a utilizar, conforme explicado na seguinte tabela:

Versão do System Manager	Termo usado para a capacidade	Tipo de capacidade referida
9.9.1 e mais tarde	Lógica utilizada	Espaço lógico utilizado se as definições de eficiência de armazenamento tiverem sido ativadas)
9,7 e 9,8	Usado	Espaço lógico utilizado (se as definições de eficiência de armazenamento tiverem sido ativadas)
9,5 e 9,6 (vista clássica)	Usado	Espaço físico utilizado

Termos de medição da capacidade

Os seguintes termos são usados ao descrever a capacidade:

- **Capacidade alocada**: A quantidade de espaço que foi alocada para volumes em uma VM de armazenamento.
- **Disponível**: A quantidade de espaço físico disponível para armazenar dados ou provisionar volumes em uma VM de storage ou em um nível local.
- **Capacidade entre volumes**: A soma do armazenamento usado e do armazenamento disponível de todos os volumes em uma VM de armazenamento.
- **Dados do cliente**: A quantidade de espaço usada pelos dados do cliente (físico ou lógico).
  - A partir do ONTAP 9.13,1, a capacidade usada pelos dados do cliente é chamada de **Logical Used**, e a capacidade usada pelas cópias Snapshot é exibida separadamente.
  - No ONTAP 9.12,1 e anterior, a capacidade usada pelos dados do cliente adicionada à capacidade usada pelas cópias Snapshot é referida como **Logical Used**.
- * Comprometido*: O montante da capacidade comprometida para um nível local.
- **Redução de dados**: A relação entre o tamanho dos dados ingeridos e o tamanho dos dados armazenados.
  - A partir do ONTAP 9.13,1, a redução de dados considera os resultados da maioria dos recursos de eficiência de storage, como deduplicação e compactação. No entanto, snapshots e thin Provisioning não são contados como parte da taxa de redução de dados.
  - No ONTAP 9.12,1 e anteriores, as relações de redução de dados são apresentadas da seguinte forma:
    - O valor de redução de dados exibido no painel **capacidade** é a proporção geral de todo o espaço lógico usado em comparação com o espaço físico usado, e inclui os benefícios derivados do uso de cópias Snapshot e outros recursos de eficiência de storage.
    - Quando você exibe o painel de detalhes, você vê a proporção **geral** exibida no painel de visão geral e a proporção do espaço lógico usado somente pelos dados do cliente em comparação com o espaço físico usado somente pelos dados do cliente, conhecido como **sem cópias Snapshot e clones**.

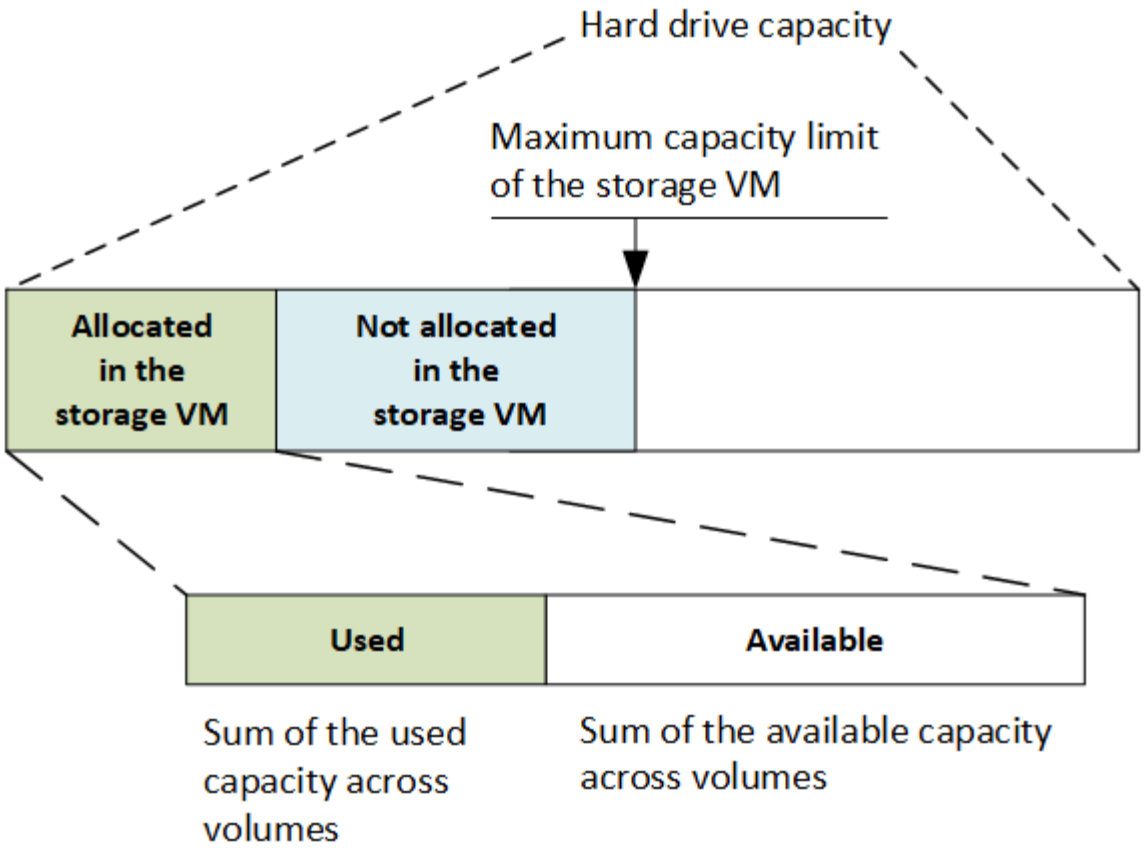
- **Utilização lógica**:
  - A partir do ONTAP 9.13,1, a capacidade usada pelos dados do cliente é chamada de **Logical Used**, e a capacidade usada pelas cópias Snapshot é exibida separadamente.
  - No ONTAP 9.12,1 e anterior, a capacidade usada pelos dados do cliente adicionada à capacidade usada pelas cópias Snapshot é referida como **uso lógico**.
- **% De utilização lógica**: A percentagem da capacidade lógica utilizada atual em comparação com o tamanho provisionado, excluindo reservas de instantâneos. Esse valor pode ser superior a 100%, pois inclui economia de eficiência no volume.
- **Capacidade máxima**: A quantidade máxima de espaço alocada para volumes em uma VM de armazenamento.
- **Físico usado**: A quantidade de capacidade usada nos blocos físicos de um volume ou nível local.
- * % Física usada*: A porcentagem de capacidade usada nos blocos físicos de um volume em comparação com o tamanho provisionado.
- **Capacidade provisionada**: Um sistema de arquivos (volume) que foi alocado de um sistema Cloud Volumes ONTAP e está pronto para armazenar dados de usuário ou aplicativo.
- **Reservado**: A quantidade de espaço reservado para volumes já provisionados em um nível local.
- **Usado**: A quantidade de espaço que contém dados.
- **Usado e reservado**: A soma do espaço físico utilizado e reservado.

Capacidade de uma VM de storage

A capacidade máxima de uma VM de armazenamento é determinada pelo espaço total alocado para volumes mais o espaço não alocado restante.

- O espaço alocado para volumes é a soma da capacidade usada e a soma da capacidade disponível dos volumes FlexVol, volumes FlexGroup e volumes FlexCache.
- A capacidade dos volumes está incluída nas somas, mesmo quando elas estão restritas, offline ou na fila de recuperação após a exclusão.
- Se os volumes estiverem configurados com crescimento automático, o valor máximo de dimensionamento automático do volume será usado nas somas. Sem crescimento automático, a capacidade real do volume é usada nas somas.

O gráfico a seguir explica como a medição da capacidade entre volumes se relaciona com o limite máximo de capacidade.



A partir do ONTAP 9.13,1, os administradores de cluster podem "Habilite um limite máximo de capacidade para uma VM de storage". No entanto, os limites de storage não podem ser definidos para uma VM de storage que contenha volumes para proteção de dados, em um relacionamento com a SnapMirror ou em uma configuração do MetroCluster. Além disso, as cotas não podem ser configuradas para exceder a capacidade máxima de uma VM de armazenamento.

Depois de definir o limite máximo de capacidade, não pode ser alterado para um tamanho inferior à capacidade atualmente alocada.

Quando uma VM de armazenamento atinge seu limite máximo de capacidade, certas operações não podem ser executadas. O System Manager fornece sugestões para as próximas etapas no **"Insights"**.

Unidades de medição da capacidade

O System Manager calcula a capacidade de armazenamento com base em unidades binárias de 1024 (2,10) bytes.

- A partir do ONTAP 9.10,1, as unidades de capacidade de armazenamento são exibidas no System Manager como KiB, MIB, GiB, TIB e PIB.
- No ONTAP 9.10,0 e anterior, essas unidades são exibidas no Gerenciador de sistema como KB, MB, GB, TB e PB.

As unidades usadas no Gerenciador de sistemas para taxa de transferência continuam a ser KB/s, MB/s, GB/s, TB/s e PB/s para todas as versões do ONTAP.

Unidade de capacidade exibida no Gerenciador do sistema para ONTAP 9.10,0 e anterior	Unidade de capacidade exibida no Gerenciador do sistema para ONTAP 9.10,1 e posterior	Cálculo	Valor em bytes
KB	KiB	1024	1024 bytes
MB	MIB	1024 * 1024	1.048.576 bytes
GB	Gib	1024 * 1024 * 1024	1.073.741.824 bytes
TB	TIB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes
PB	PIB	1024 * 1024 * 1024 * 1024 * 1024	1.125.899.906.842.624 bytes

Informações relacionadas

"Monitorar a capacidade no System Manager"

"Relatórios de espaço lógico e imposição para volumes"

Visão geral da eficiência de storage sensível à temperatura

O ONTAP fornece benefícios de eficiência de storage sensíveis à temperatura ao avaliar a frequência com que os dados do volume são acessados e mapear essa frequência para o nível de compressão aplicado a esses dados. Para dados inativos acessados com pouca frequência, blocos de dados maiores são compatados e, para dados ativos, acessados com frequência e substituídos com mais frequência, blocos de dados menores são compatados, tornando o processo mais eficiente.

A eficiência de storage sensível à temperatura (SSE) é introduzida no ONTAP 9.8 e é ativada automaticamente em volumes AFF recém-criados com provisionamento reduzido. Você pode ativar a eficiência de storage sensível à temperatura em volumes AFF existentes e em volumes DP não AFF provisionados de forma fina.

> A eficiência de storage sensível à temperatura não é aplicada nas plataformas AFF A70, AFF A90 e AFF A1K. A compactação não se baseia em dados ativos ou inativos nessas plataformas. Portanto, a compactação começa sem esperar que os dados fiquem inativos.

Introdução dos modos "padrão" e "eficiente"

A partir do ONTAP 9.10,1, os modos de eficiência de storage no nível de volume *default* e *efficient* são introduzidos apenas para sistemas AFF. Os dois modos oferecem a opção entre compactação de arquivos (padrão), que é o modo padrão ao criar novos volumes AFF ou eficiência de storage sensível à temperatura (eficiente), que permite a eficiência de storage sensível à temperatura. Com o ONTAP 9.10,1, "a eficiência de storage sensível à temperatura deve ser definida explicitamente" para ativar a compressão adaptável automática. No entanto, outros recursos de eficiência de storage, como compactação de dados, cronograma de deduplicação automática, deduplicação in-line entre volumes e deduplicação em segundo plano entre volumes, são habilitados por padrão nas plataformas AFF para os modos padrão e eficiente.

Ambos os modos de eficiência de storage (padrão e eficiente) são compatíveis com agregados habilitados para FabricPool e com todos os tipos de política de disposição em camadas.

Eficiência de storage sensível à temperatura ativada nas plataformas C-Series

A eficiência de storage sensível à temperatura é habilitada por padrão nas plataformas AFF C-Series e ao migrar volumes de uma plataforma que não seja TSSE para uma plataforma C-Series habilitada para TSSE usando a movimentação de volume ou SnapMirror com as seguintes versões instaladas no destino:

- ONTAP 9.12.1P4 e posterior
- ONTAP 9.13,1 e posterior

Para obter mais informações, "Comportamento de eficiência de storage com movimentação de volume e operações de SnapMirror"consulte .

No caso dos volumes existentes, a eficiência de storage sensível à temperatura não é ativada automaticamente. No entanto, é possível "modificar o modo de eficiência de storage"alterar manualmente para o modo eficiente.

> Depois de alterar o modo de eficiência de storage para eficiente, você não poderá alterá-lo novamente.

Eficiência de storage aprimorada com embalagem sequencial de blocos físicos contíguos

A partir do ONTAP 9.13,1, a eficiência de storage sensível à temperatura adiciona empacotamento sequencial de blocos físicos contíguos para aprimorar ainda mais a eficiência de storage. Os volumes que têm a eficiência de storage sensível à temperatura ativada automaticamente têm o empacotamento sequencial habilitado quando você atualiza os sistemas para o ONTAP 9.13,1. Depois que a embalagem sequencial estiver ativada, é "reembalar manualmente os dados existentes"necessário .

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1 e posterior, os volumes existentes recebem um modo de eficiência de storage com base no tipo de compactação atualmente habilitado nos volumes. Durante uma atualização, os volumes com compressão ativada recebem o modo padrão e os volumes com eficiência de storage sensível à temperatura ativada recebem o modo eficiente. Se a compactação não estiver ativada, o modo de eficiência de storage permanecerá em branco.

CPU ou eficiência de storage do processador de descarga dedicado

A partir do ONTAP 9.15,1, o ONTAP oferece eficiência de storage e compactação de dados nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90.

Dependendo da plataforma, o seguinte se aplica ao atualizar:

- A compactação é realizada usando a CPU principal ou com um processador de descarga dedicado.
- A eficiência de storage é habilitada por padrão em todos os volumes com thin Provisioning ou apenas volumes existentes.

  Para uma plataforma FF A70, AFF A90 ou AFF A1K, a eficiência de storage é ativada automaticamente e não requer configuração. Isso se aplica a todos os volumes thin Provisioning e dados existentes recentemente criados, incluindo volumes movidos de outras plataformas para uma plataforma AFF A70, AFF A90 ou AFF A1K.

  Para uma plataforma FAS70 ou FAS90, a eficiência de storage é habilitada por padrão somente nos

volumes thin Provisioning existentes que tiveram a eficiência de storage habilitada antes da atualização. Você pode ativar a eficiência de storage em volumes criados recentemente usando o método de CLI ou API REST.

- Os dados migrados usando a tecnologia de movimentação de volume ou SnapMirror são convertidos automaticamente para compactação in-line de 32k TB:

  Para uma plataforma AFF A70, AFF A90 ou AFF A1K, os dados são convertidos automaticamente.

  Para uma plataforma FAS70 ou FAS90, os dados são convertidos somente se a compactação foi ativada na plataforma original.

A eficiência de storage sensível à temperatura não é aplicada nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90. A compactação não se baseia em dados ativos ou inativos nessas plataformas. Portanto, a compactação começa sem esperar que os dados fiquem inativos.

A eficiência de storage nas plataformas AFF A70, AFF A90, AFF A1K, FAS70 e FAS90 usa a embalagem sequencial de blocos físicos contíguos para aprimorar ainda mais a eficiência de storage para dados compatados.

Para obter informações sobre como atualizar uma controladora para um AFF A70, AFF A90, AFF A1K, FAS70 ou FAS90, consulte "Documentação de atualização de hardware da ONTAP".

Segurança

Autenticação e autorização do cliente

O ONTAP usa métodos padrão para proteger o acesso do cliente e do administrador ao armazenamento e para proteger contra vírus. Tecnologias avançadas estão disponíveis para criptografia de dados em repouso e para storage WORM.

O ONTAP autentica uma máquina cliente e um usuário verificando suas identidades com uma fonte confiável. O ONTAP autoriza um usuário a acessar um arquivo ou diretório comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório.

Autenticação

Você pode criar contas de usuário locais ou remotas:

- Uma conta local é aquela em que as informações da conta residem no sistema de armazenamento.
- Uma conta remota é aquela em que as informações de conta são armazenadas em um controlador de domínio do ative Directory, um servidor LDAP ou um servidor NIS.

O ONTAP usa serviços de nomes locais ou externos para procurar informações de mapeamento de nome, usuário, grupo, grupo netgroup e nome do host. O ONTAP oferece suporte aos seguintes serviços de nomes:

- Usuários locais
- DNS
- Domínios NIS externos
- Domínios LDAP externos

Uma tabela *name Service switch* especifica as fontes para procurar informações de rede e a ordem na qual

pesquisá-las (fornecendo a funcionalidade equivalente do arquivo /etc/nsswitch.conf em sistemas UNIX). Quando um cliente nas se coneta ao SVM, o ONTAP verifica os serviços de nome especificados para obter as informações necessárias.

Kerberos support Kerberos é um protocolo de autenticação de rede que fornece "autenticação de conexão", criptografando senhas de usuário em implementações cliente-servidor. O ONTAP suporta autenticação Kerberos 5 com verificação de integridade (krb5i) e autenticação Kerberos 5 com verificação de privacidade (krb5p).

Autorização

O ONTAP avalia três níveis de segurança para determinar se uma entidade está autorizada a executar uma ação solicitada em arquivos e diretórios localizados em um SVM. O acesso é determinado pelas permissões efetivas após a avaliação dos níveis de segurança:

- Segurança de exportação (NFS) e compartilhamento (SMB)

  A segurança de exportação e compartilhamento se aplica ao acesso do cliente a uma determinada exportação NFS ou compartilhamento SMB. Os usuários com Privileges administrativo podem gerenciar a segurança de exportação e compartilhamento a partir de clientes SMB e NFS.

- Segurança de arquivo e diretório do Access Guard no nível de armazenamento

  A segurança do Access Guard no nível de storage se aplica ao acesso de clientes SMB e NFS aos volumes SVM. Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

- Segurança nativa em nível de arquivo NTFS, UNIX e NFSv4

  A segurança de nível de arquivo nativo existe no arquivo ou diretório que representa o objeto de storage. Você pode definir a segurança no nível do arquivo de um cliente. As permissões de arquivo são efetivas independentemente de SMB ou NFS serem usados para acessar os dados.

Autenticação com SAML

O ONTAP suporta a linguagem de marcação de asserção de Segurança (SAML) para autenticação de usuários remotos. Vários provedores de identidade populares (IDPs) são suportados. Para obter mais informações sobre IDPs suportados e instruções para ativar a autenticação SAML, "Configurar a autenticação SAML"consulte .

OAuth 2,0 com clientes API REST do ONTAP

O suporte para a estrutura de autorização aberta (OAuth 2,0) está disponível a partir do ONTAP 9.14. Você só pode usar o OAuth 2,0 para tomar decisões de autorização e controle de acesso quando o cliente usa a API REST para acessar o ONTAP. No entanto, você pode configurar e ativar o recurso com qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI, o Gerenciador de sistema e a API REST.

Os recursos padrão do OAuth 2,0 são suportados juntamente com vários servidores de autorização populares. Você pode aprimorar ainda mais a segurança do ONTAP usando tokens de acesso restritos ao remetente baseados no TLS mútuo. E há uma ampla variedade de opções de autorização disponíveis, incluindo escopos autônomos, bem como integração com as funções REST do ONTAP e definições de usuário local. Consulte "Visão geral da implementação do ONTAP OAuth 2,0" para obter mais informações.

Autenticação de administrador e RBAC

Os administradores usam contas de login locais ou remotas para se autenticar no cluster e na SVM. O controle de acesso baseado em função (RBAC) determina os comandos aos quais um administrador tem acesso.

Autenticação

Você pode criar contas de administrador de cluster local ou remoto e SVM:

- Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento.
- Uma conta remota é aquela em que as informações de conta são armazenadas em um controlador de domínio do ative Directory, um servidor LDAP ou um servidor NIS.

Exceto o DNS, o ONTAP usa os mesmos serviços de nome para autenticar contas de administrador que ele usa para autenticar clientes.

RBAC

A *função* atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Verificação de vírus

Você pode usar a funcionalidade de antivírus integrada no sistema de armazenamento para proteger os dados contra o comprometimento por vírus ou outros códigos maliciosos. A verificação de vírus do ONTAP, chamada *Vscan*, combina o melhor software antivírus de terceiros com recursos do ONTAP que oferecem a flexibilidade necessária para controlar quais arquivos são verificados e quando.

Os sistemas de storage descarregam as operações de verificação para servidores externos que hospedam softwares antivírus de terceiros. O *ONTAP Antivirus Connector*, fornecido pelo NetApp e instalado no servidor externo, lida com as comunicações entre o sistema de armazenamento e o software antivírus.

- Você pode usar *verificação no acesso* para verificar se há vírus quando os clientes abrem, leem, renomeam ou fecham arquivos pelo SMB. A operação do arquivo é suspensa até que o servidor externo comunique o status da digitalização do arquivo. Se o ficheiro já tiver sido lido, o ONTAP permite a operação do ficheiro. Caso contrário, ele solicita uma verificação do servidor.

  A verificação no acesso não é suportada para NFS.

- Você pode usar *On-demand scanning* para verificar arquivos para vírus imediatamente ou em uma programação. Por exemplo, você pode querer executar digitalizações apenas em horas fora de pico. O servidor externo atualiza o status de verificação dos arquivos verificados, de modo que a latência de acesso ao arquivo desses arquivos (supondo que eles não tenham sido modificados) seja normalmente reduzida quando forem acessados pela próxima vez por SMB.

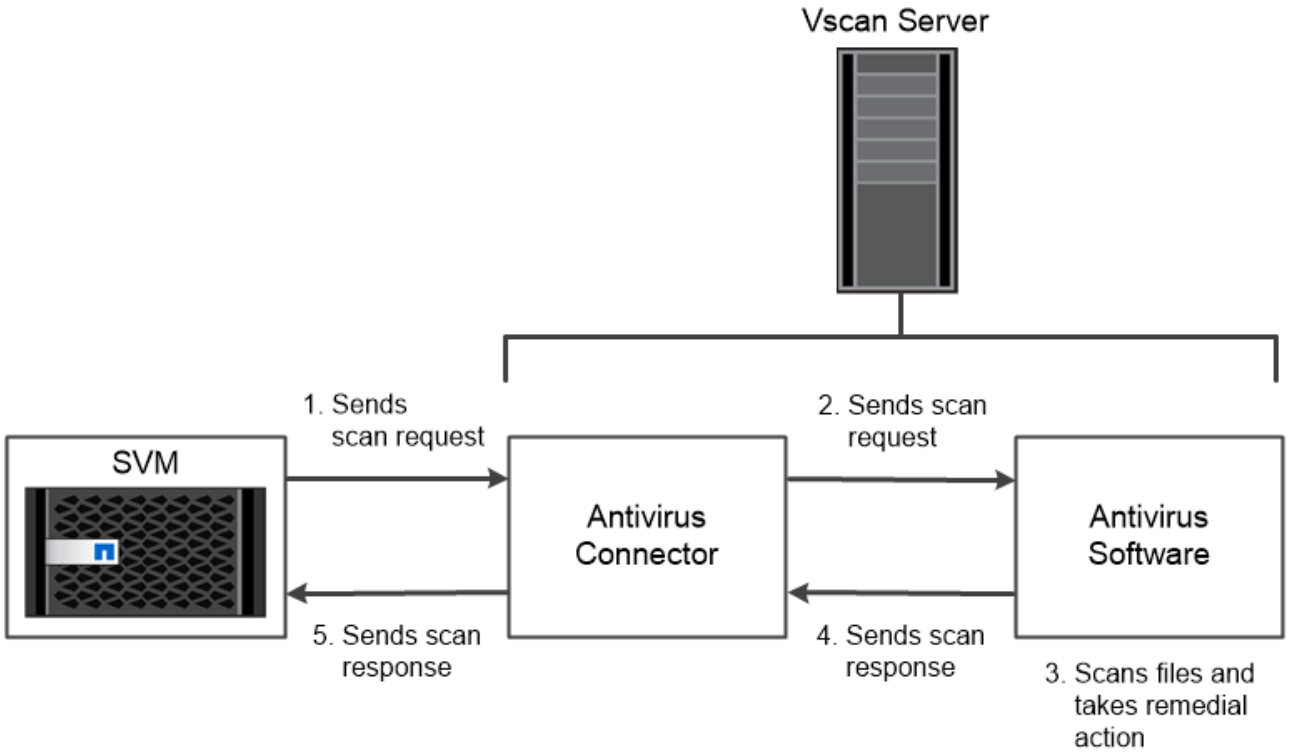
  Você pode usar a verificação sob demanda para qualquer caminho no namespace SVM, até mesmo para volumes exportados somente por NFS.

Normalmente, você ativa ambos os modos de digitalização em um SVM. Em ambos os modos, o software

antivírus toma medidas corretivas em arquivos infetados com base em suas configurações no software.

Verificação de vírus na recuperação de desastres e configurações do MetroCluster

Para a recuperação de desastres e configurações do MetroCluster, é necessário configurar servidores Vscan separados para os clusters locais e parceiros.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Criptografia

A ONTAP oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode usar as seguintes soluções de criptografia:

- Soluções de hardware:
  - Criptografia de storage do NetApp (NSE)

    O NSE é uma solução de hardware que usa unidades de autocriptografia (SEDs).
  - SEDs NVMe

    O ONTAP fornece criptografia completa de disco para SEDs NVMe que não têm a certificação FIPS 140-2-2.

- Soluções de software:
  - Criptografia de agregados NetApp (NAE)

    NAE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele é habilitado com chaves exclusivas para cada agregado.

  - Criptografia de volume NetApp (NVE)

    O NVE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade em que ele esteja habilitado com uma chave exclusiva para cada volume.

Use as soluções de criptografia de software (NAE ou NVE) e hardware (NSE ou NVMe SED) para obter criptografia dupla em repouso. A eficiência de storage não é afetada pela criptografia NVE ou NAE.

Criptografia de storage do NetApp

O NetApp Storage Encryption (NSE) é compatível com SEDs que criptografam dados à medida que são gravados. Os dados não podem ser lidos sem uma chave de criptografia armazenada no disco. A chave de criptografia, por sua vez, é acessível apenas para um nó autenticado.

Em uma solicitação de e/S, um nó se autentica em uma SED usando uma chave de autenticação recuperada de um servidor de gerenciamento de chaves externo ou Gerenciador de chaves integrado:

- O servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que fornece chaves de autenticação para nós que usam o Key Management Interoperability Protocol (KMIP).
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados.

O NSE é compatível com HDDs e SSDs com autocriptografia. Você pode usar a criptografia de volume NetApp com NSE para criptografar dados duas vezes em unidades NSE.

Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Unidades com autocriptografia NVMe

No entanto, esses discos usam a criptografia de disco transparente AES de 256 bits para proteger os dados em repouso 140-2.

As operações de criptografia de dados, como a geração de uma chave de autenticação, são realizadas internamente. A chave de autenticação é gerada na primeira vez que o disco é acessado pelo sistema de armazenamento. Depois disso, os discos protegem os dados em repouso exigindo autenticação do sistema de storage sempre que as operações de dados forem solicitadas.

Criptografia de agregados NetApp

O NetApp Aggregate Encryption (NAE) é uma tecnologia baseada em software para criptografar todos os dados em um agregado. Um benefício do NAE é que os volumes estão incluídos na deduplicação de nível agregado, enquanto os volumes NVE são excluídos.

Com o NAE ativado, os volumes dentro do agregado podem ser criptografados com chaves agregadas.

A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você tem o "Licença NVE" e gerenciamento de chaves externas ou integradas.

Criptografia de volume do NetApp

O NetApp volume Encryption (NVE) é uma tecnologia baseada em software para criptografar dados em repouso, um volume de cada vez. Uma chave de criptografia acessível apenas para o sistema de armazenamento garante que os dados de volume não possam ser lidos se o dispositivo subjacente for separado do sistema.

Os dados, incluindo cópias Snapshot, e metadados, são criptografados. O acesso aos dados é dado por uma chave exclusiva XTS-AES-256, uma por volume. Um Gerenciador de chaves integrado protege as chaves no mesmo sistema com seus dados.

Você pode usar o NVE em qualquer tipo de agregado (HDD, SSD, híbrido, LUN de array), com qualquer tipo de RAID e em qualquer implementação de ONTAP com suporte, incluindo ONTAP Select. Você também pode usar o NVE com criptografia de storage NetApp (NSE) para criptografar dados duas vezes em unidades NSE.

quando usar servidores KMIP embora seja menos caro e normalmente mais conveniente usar o Gerenciador de chaves integrado, você deve configurar servidores KMIP se qualquer uma das seguintes situações for verdadeira:

- Sua solução de gerenciamento de chaves de criptografia precisa estar em conformidade com Federal Information Processing Standards (FIPS) 140-2 ou com o padrão OASIS KMIP.
- Você precisa de uma solução de vários clusters. Os servidores KMIP são compatíveis com vários clusters com gerenciamento centralizado de chaves de criptografia.

  Os servidores KMIP são compatíveis com vários clusters com gerenciamento centralizado de chaves de criptografia.

- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

  Os servidores KMIP armazenam as chaves de autenticação separadamente dos dados.

Informações relacionadas

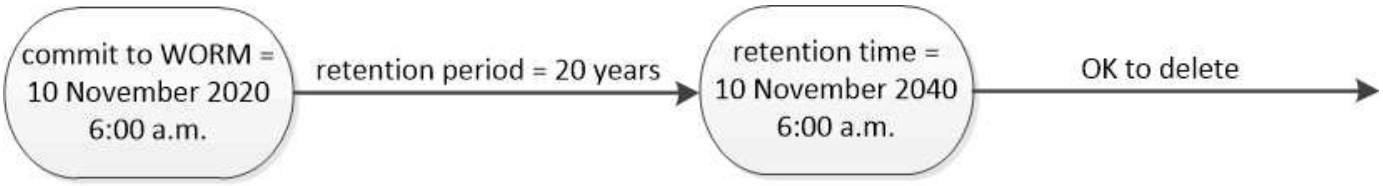
"Perguntas frequentes - encriptação de volume NetApp e encriptação agregada NetApp"

STORAGE WORM

O *SnapLock* é uma solução de conformidade de alto desempenho para organizações que usam o armazenamento *write once, read many (WORM)* para reter arquivos críticos de forma não modificada para fins regulatórios e de governança.

Uma única licença permite que você use o SnapLock no estrito modo *Compliance,* para satisfazer mandatos externos, como a regra SEC 17a-4(f), e um modo *Enterprise mais solto,* para atender aos regulamentos internos exigidos para a proteção de ativos digitais. O SnapLock usa um *ComplianceClock* à prova de violação para determinar quando o período de retenção de um arquivo WORM tiver decorrido.

Use o *SnapLock for SnapVault* para proteger cópias Snapshot WORM no storage secundário. Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres e outros fins.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAP e VMware vSphere

Você pode integrar o ONTAP e os produtos relacionados do NetApp com o VMware vSphere. Existem várias opções disponíveis, dependendo do ambiente de tecnologia e das necessidades do seu negócio.

Conceitos e terminologia selecionados

À medida que você começa a explorar o uso do ONTAP e de produtos NetApp relacionados em um ambiente VMware, é útil primeiro conhecer alguns dos principais conceitos e terminologia.

Número de unidade lógica

Um LUN é um número usado para identificar uma *unidade lógica* dentro de uma SAN (Storage Area Network). Esses dispositivos endereçáveis são normalmente discos lógicos acessados através do protocolo SCSI (Small Computer System Interface) ou de um de seus derivados encapsulados.

Volume virtual do VMware vSphere

Um volume virtual (vVol) fornece uma abstração em nível de volume para o storage usado por uma máquina virtual. Ele inclui vários benefícios e fornece uma alternativa ao uso de um LUN tradicional.

Reservas persistentes

As reservas persistentes são suportadas com SCSI-3 e uma melhoria em relação às reservas SCSI-2 anteriores. Eles permitem que vários iniciadores de cliente se comuniquem com um único destino enquanto bloqueiam outros nós. As reservas podem persistir mesmo que o barramento seja redefinido para recuperação de erros.

> ⓘ A partir do ONTAP 9.15,1, você pode criar uma reserva persistente para um volume virtual usando SCSI-3. Esse recurso só é compatível com o uso das Ferramentas do ONTAP para VMware vSphere 9 com um cluster de failover de servidor do Windows (WSFC).

Cluster de failover do Windows Server

O Microsoft WSFC é um recurso do sistema operacional Windows Server que fornece tolerância a falhas e alta disponibilidade. Um conjunto de nós de servidor (físicos ou virtuais) é Unido como um cluster para fornecer resiliência em caso de falha. O WSFC é comumente usado para implantar serviços de infraestrutura, incluindo servidores de banco de dados, arquivos e namespaces.

VMware vSphere Storage APIs - Storage Awareness

O VASA é um conjunto de APIs que fornecem integração dos storage arrays com o vCenter para gerenciamento e administração. A arquitetura é baseada em vários componentes, incluindo o *VASA Provider*, que lida com a comunicação entre o VMware vSphere e os sistemas de armazenamento. Com o ONTAP, o provedor é implementado como parte das ferramentas do ONTAP para o VMware vSphere.

VMware vSphere Storage APIs - Array Integration

O VAAI é um conjunto de APIs que permitem a comunicação entre os hosts do VMware vSphere ESXi e os dispositivos de armazenamento. A API inclui um conjunto de operações primitivas usadas pelos hosts para descarregar operações de storage para o array. O VAAI pode fornecer melhorias significativas de desempenho para tarefas com uso intenso de storage.

NetApp SnapCenter

O SnapCenter é uma plataforma centralizada e dimensionável que fornece proteção de dados para aplicações, bancos de dados, sistemas de arquivos host e máquinas virtuais que usam sistemas de storage ONTAP. Ele utiliza as tecnologias nativas da ONTAP, incluindo Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault.

Plug-ins do NetApp e tecnologias relacionadas

O NetApp fornece suporte robusto para a integração do ONTAP e produtos relacionados com as tecnologias VMware vSphere.

Ferramentas do ONTAP para VMware vSphere

As ferramentas do ONTAP para VMware vSphere são um conjunto de ferramentas para integrar o ONTAP e o vSphere. Ele implementa a funcionalidade do provedor da estrutura da API VASA. As ferramentas do ONTAP também incluem o plug-in do vCenter, um adaptador de replicação de storage (SRA) para o VMware Site Recovery Manager e um servidor de API REST que você pode usar para criar aplicativos de automação.

Plug-in NFS para VMware VAAI

O plug-in NFS do NetApp para VMware VAAI fornece acesso aos recursos do VAAI. O plug-in pode ser instalado em hosts ESXi e permite que os hosts aproveitem o VAAI com os datastores NFS no ONTAP. Ele fornece várias operações, incluindo clonagem, reservas de espaço e descarregamento de snapshot.

VMware Site Recovery Manager

O VMware Site Recovery Manager (SRM) fornece uma capacidade de recuperação de desastres. O SRM se integra às ferramentas do ONTAP para o VMware vSphere acessar e aproveitar a funcionalidade de gerenciamento de dados do ONTAP.

Cluster de armazenamento vSphere Metro

O vSphere Metro Storage Cluster (vmsc) é uma tecnologia que permite e suporta o vSphere em uma implantação de cluster *estendido*. As soluções vmsc são compatíveis com o NetApp MetroCluster e o SnapMirror ative Sync (anteriormente SMBC). Essas soluções fornecem continuidade de negócios aprimorada em caso de falha de domínio. O modelo de resiliência é baseado em suas escolhas de configuração específicas.

Plug-in do SnapCenter para VMware vSphere

O plug-in do SnapCenter para VMware vSphere (SCV) é um dispositivo virtual baseado em Linux que você pode implantar em conjunto com o servidor SnapCenter ou como um aplicativo autônomo. Em ambos os casos, o SCV fornece operações de backup e restauração de VMs, armazenamentos de dados e VMDKs. As operações são rápidas, com uso eficiente de espaço, consistentes com falhas e consistentes com VM.

Obtenha mais informações

Há vários recursos adicionais disponíveis para ajudá-lo a se preparar para implantar o ONTAP em um

ambiente VMware vSphere.

- "Ferramentas do ONTAP para documentação do VMware vSphere"
- "Aplicações empresariais: VMware vSphere com ONTAP"
- "NetApp KB: O que são Reservas SCSI e Reservas persistentes SCSI?"
- "Plug-in do SnapCenter para documentação do VMware vSphere"

Gerenciamento de dados com reconhecimento de aplicações

O gerenciamento de dados com reconhecimento de aplicações permite descrever o aplicativo que você deseja implantar no ONTAP em termos de aplicativo, em vez de em termos de storage. O aplicativo pode ser configurado e pronto para servir dados rapidamente com o mínimo de entradas usando o System Manager e as APIs REST.

O recurso de gerenciamento de dados com reconhecimento de aplicações fornece uma maneira de configurar, gerenciar e monitorar o storage no nível de aplicativos individuais. Esse recurso incorpora práticas recomendadas relevantes da ONTAP para provisionar aplicações de forma otimizada, com posicionamento equilibrado de objetos de storage com base nos níveis de serviço de performance desejados e nos recursos do sistema disponíveis.

O recurso de gerenciamento de dados com reconhecimento de aplicativo inclui um conjunto de modelos de aplicativo, com cada modelo composto por um conjunto de parâmetros que descrevem coletivamente a configuração de um aplicativo. Esses parâmetros, que geralmente são predefinidos com valores padrão, definem as caraterísticas que um administrador de aplicativos poderia especificar para provisionar armazenamento em um sistema ONTAP, como tamanhos de banco de dados, níveis de serviço, elementos de acesso de protocolo, como LIFs, bem como critérios de proteção locais e critérios de proteção remota. Com base nos parâmetros especificados, o ONTAP configura entidades de storage, como LUNs e volumes, com tamanhos e níveis de serviço apropriados para a aplicação.

Você pode executar as seguintes tarefas para seus aplicativos:

- Crie aplicativos usando os modelos de aplicativo
- Gerenciar o armazenamento associado aos aplicativos
- Modificar ou eliminar as aplicações
- Ver aplicações
- Gerenciar cópias Snapshot das aplicações
- Crie grupos de consistência para fornecer funcionalidades de proteção de dados selecionando vários LUNs nos mesmos volumes ou em volumes diferentes

FabricPool

Muitos clientes da NetApp têm quantidades significativas de dados armazenados que raramente são acessados. Chamamos isso de *cold* dados. Os clientes também têm dados que são acessados com frequência, que chamamos de *hot* data. Idealmente, você deseja manter seus dados ativos em seu storage mais rápido para obter a melhor performance. Os dados inativos podem se mover para um armazenamento mais lento, desde que estejam imediatamente disponíveis, se necessário. Mas como você sabe quais partes de seus dados estão quentes e quais são frios?

O FabricPool é um recurso do ONTAP que move dados automaticamente entre uma camada local (agregado) de alta performance e uma camada de nuvem com base em padrões de acesso. A disposição em categorias libera espaço no storage local caro para os dados ativos enquanto mantém os dados inativos prontamente disponíveis no storage de objetos de baixo custo na nuvem. O FabricPool monitora constantemente o acesso aos dados e migra os dados entre as camadas para melhor performance e máxima economia.

Usar o FabricPool para categorizar dados pouco acessados na nuvem é uma das maneiras mais fáceis de ganhar eficiência e criar uma configuração de nuvem híbrida. O FabricPool trabalha em nível de bloco de storage, portanto, trabalha com dados LUN e de arquivo.

No entanto, o FabricPool não se destina apenas a separar os dados on-premises para a nuvem. Muitos clientes usam o FabricPool em Cloud Volumes ONTAP para categorizar dados inativos de storage de nuvem mais caro para storage de objetos de baixo custo dentro do fornecedor de nuvem. A partir do ONTAP 9.8, é possível capturar análises em volumes habilitados para FabricPool com "Análise do sistema de arquivos" ou "eficiência de storage sensível à temperatura".

As aplicações que usam os dados não sabem que eles estão dispostos em categorias, portanto, não são necessárias alterações nas aplicações. A disposição em camadas é totalmente automática, portanto, não é necessária administração contínua.

Você pode armazenar dados inativos no storage de objetos de um dos principais fornecedores de nuvem. Ou escolha a NetApp StorageGRID para manter seus dados inativos na sua própria nuvem privada, proporcionando a melhor performance e controle total sobre seus dados.

Informações relacionadas

"Doc do Gestor de sistema FabricPool"

"Disposição em camadas do BlueXP"

"Lista de reprodução do FabricPool na NetApp TechComm TV"

Integração do System Manager com o BlueXP

A partir do ONTAP 9.12,1, o Gerenciador de sistema é totalmente integrado ao BlueXP . Com o BlueXP , você pode gerenciar sua infraestrutura multicloud híbrida a partir de um único painel de controle enquanto mantém o já conhecido painel do System Manager.

O BlueXP permite que você crie e administre armazenamento em nuvem (por exemplo, Cloud Volumes ONTAP), use os serviços de dados do NetApp (por exemplo, backup em nuvem) e controle muitos dispositivos de armazenamento no local e na borda.

Para usar o Gerenciador de sistema no BlueXP , execute as seguintes etapas:

Passos

1. Abra um navegador da Web e insira o endereço IP da interface de rede de gerenciamento de cluster.

   Se o cluster tiver conetividade com o BlueXP , será exibido um prompt de login.

2. Clique em **Continue to BlueXP** para seguir o link para BlueXP .

Se as configurações do sistema bloquearam redes externas, você não poderá acessar o BlueXP . Para acessar o Gerenciador de sistema usando o BlueXP , você deve garantir que o endereço "'cloudmanager.cloud.NetApp.com'" possa ser acessado pelo seu sistema. Caso contrário, no prompt, você pode optar por usar a versão do Gerenciador de sistema que está instalada com seu sistema ONTAP.

3. Na página de login do BlueXP , selecione **Faça login com suas credenciais do site de suporte da NetApp** e insira suas credenciais.

   Se você já usou o BlueXP e tem um login usando um e-mail e senha, então você precisará continuar usando essa opção de login.

   "Saiba mais sobre como fazer login no BlueXP ".

4. Se você for solicitado, insira um nome para sua nova conta do BlueXP .

   Na maioria dos casos, o BlueXP cria automaticamente uma conta para você com base nos dados do cluster.

5. Insira as credenciais de administrador do cluster para o cluster.

Resultado

O Gerenciador do sistema é exibido e agora você pode gerenciar o cluster a partir do BlueXP .

Descubra seus clusters diretamente do BlueXP

O BlueXP oferece duas maneiras de descobrir e gerenciar clusters:

- Descoberta direta para gerenciamento por meio do System Manager

  Esta é a mesma opção de descoberta descrita na seção anterior com a qual você segue o redirecionamento.

- Descoberta através de um conetor

  O Connector é um software instalado no seu ambiente que permite acessar funções de gerenciamento por meio do System Manager e também acessar serviços de nuvem da BlueXP que fornecem recursos como replicação de dados, backup e recuperação, classificação de dados, disposição em categorias de dados e muito mais.

Vá para a "Documentação do BlueXP" para saber mais sobre essas opções de descoberta e gerenciamento.

Saiba mais sobre o BlueXP

- "Visão geral do BlueXP "
- "Gerencie seus sistemas NetApp AFF e FAS por meio do BlueXP "

Configure, atualize e reverta o software e o firmware do ONTAP

Configure o ONTAP

Comece a configurar o cluster do ONTAP

Use o Gerenciador do sistema ou a interface de linha de comando (CLI) do ONTAP para configurar novos clusters do ONTAP. Antes de começar, você deve coletar as informações necessárias para concluir a configuração do cluster, como a porta da interface de gerenciamento de cluster e o endereço IP.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para configurar um cluster ONTAP. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A NetApp recomenda que "Use o System Manager para configurar novos clusters"você . O System Manager fornece um fluxo de trabalho simples e fácil para configuração e configuração de cluster, incluindo a atribuição de um endereço IP de gerenciamento de nós, a inicialização do cluster, a criação de um nível local, a configuração de protocolos e o provisionamento de armazenamento inicial.

Só é necessário "Use a CLI do ONTAP para configurar o cluster" se você estiver executando o ONTAP 9.7 ou anterior em uma configuração do MetroCluster.

A partir do ONTAP 9.13,1, nas plataformas AFF A800 e FAS8700, você também pode usar a CLI ONTAP para criar e configurar novos clusters em ambientes de rede somente IPv6. Se precisar usar o IPv6 no ONTAP 9.13,0 e anterior ou em outras plataformas no ONTAP 9.13,1 e posterior, use o Gerenciador do sistema para criar novos clusters usando o IPv4 e "Converter para IPv6"o .

O que você precisará para a configuração do cluster

A configuração do cluster envolve a coleta das informações necessárias para configurar a configuração de cada nó, a criação do cluster no primeiro nó e a junção de todos os nós restantes ao cluster.

Comece reunindo todas as informações relevantes nas planilhas de configuração do cluster.

A folha de cálculo de configuração do cluster permite-lhe registar os valores de que necessita durante o processo de configuração do cluster. Se um valor padrão for fornecido, você pode usar esse valor ou então digitar o seu próprio.

Predefinições do sistema

Os padrões do sistema são os valores padrão para a rede de cluster privada. É melhor usar esses valores padrão. No entanto, se eles não atenderem aos seus requisitos, você pode usar a tabela para Registrar seus próprios valores.

Para clusters configurados para usar switches de rede, cada switch de cluster deve usar o tamanho de MTU 9000.

Tipos de informação	Seus valores
Portas de rede de cluster privado	
Máscara de rede de cluster	
Endereços IP da interface de cluster (para cada porta de rede de cluster em cada nó) os endereços IP de cada nó devem estar na mesma sub-rede.	

Informações do cluster

Tipos de informação	Seus valores
Nome do cluster o nome deve começar com uma letra e deve ter menos de 44 carateres. O nome pode incluir os seguintes carateres especiais: . - _	

Chaves de licença de recurso

Você pode encontrar chaves de licença para seus pedidos de software iniciais ou complementares no site de suporte da NetApp em **meu suporte** > **licenças de software**.

Tipos de informação	Seus valores
Chaves de licença de recurso	

Máquina virtual de storage de administração (SVM)

Tipos de informação	Seus valores
Senha do administrador do cluster A senha da conta de administrador que o cluster exige antes de conceder acesso ao console pelo administrador do cluster ou por meio de um protocolo seguro. Para fins de segurança, a gravação de senhas nesta Planilha não é recomendada. As regras padrão para senhas são as seguintes: • Uma senha deve ter pelo menos oito carateres. • Uma senha deve conter pelo menos uma letra e um número.	

Tipos de informação	Seus valores
Porta de interface de gerenciamento de clusters A porta física que está conetada à rede de dados e permite que o administrador do cluster gerencie o cluster.	
Endereço IP da interface de gerenciamento de cluster Um endereço IPv4 ou IPv6 exclusivo para a interface de gerenciamento de cluster. O administrador do cluster usa esse endereço para acessar o administrador SVM e gerenciar o cluster. Normalmente, esse endereço deve estar na rede de dados. Você pode obter esse endereço IP do administrador responsável pela atribuição de endereços IP na sua organização. Exemplo: 192.0.2.66	
Máscara de rede de interface de gerenciamento de cluster (IPv4) A máscara de sub-rede que define o intervalo de endereços IPv4 válidos na rede de gerenciamento de cluster. Exemplo: 255.255.255.0	
Comprimento da máscara de rede da interface de gerenciamento de cluster (IPv6) Se a interface de gerenciamento de cluster usar um endereço IPv6, esse valor representa o comprimento do prefixo que define o intervalo de endereços IPv6 válidos na rede de gerenciamento de cluster. Exemplo: 64	
Gateway padrão da interface de gerenciamento de cluster O endereço IP do roteador na rede de gerenciamento de cluster.	

Tipos de informação	Seus valores
Nome de domínio DNS O nome do domínio DNS da rede. O nome de domínio deve consistir em carateres alfanuméricos. Para inserir vários nomes de domínio DNS, separe cada nome com uma vírgula ou um espaço.	
Endereços IP do servidor de nomes Os endereços IP dos servidores de nomes DNS. Separe cada endereço com uma vírgula ou um espaço.	

Informações do nó (para cada nó no cluster)

Tipos de informação	Seus valores
Localização física do controlador (opcional) Uma descrição da localização física do controlador. Use uma descrição que identifique onde encontrar esse nó no cluster (por exemplo, "'Lab 5, Row 7, Rack B'").	
Porta de interface de gerenciamento de nó A porta física que está conetada à rede de gerenciamento de nós e permite que o administrador do cluster gerencie o nó.	
Endereço IP da interface de gerenciamento do nó Um endereço IPv4 ou IPv6 exclusivo para a interface de gerenciamento de nós na rede de gerenciamento. Se você definiu a porta da interface de gerenciamento de nó como uma porta de dados, esse endereço IP deve ser um endereço IP exclusivo na rede de dados. Você pode obter esse endereço IP do administrador responsável pela atribuição de endereços IP na sua organização. Exemplo: 192.0.2.66	

Tipos de informação	Seus valores
Máscara de rede de interface de gerenciamento de nó (IPv4) A máscara de sub-rede que define o intervalo de endereços IP válidos na rede de gerenciamento de nós. Se você definiu a porta de interface de gerenciamento de nó como uma porta de dados, a máscara de rede deve ser a máscara de sub-rede da rede de dados. Exemplo: 255.255.255.0	
Comprimento da máscara de rede da interface de gestão do nó (IPv6) Se a interface de gerenciamento de nó usa um endereço IPv6, esse valor representa o comprimento do prefixo que define o intervalo de endereços IPv6 válidos na rede de gerenciamento de nó. Exemplo: 64	
Gateway padrão da interface de gerenciamento de nó O endereço IP do roteador na rede de gerenciamento de nós.	

Informações do servidor NTP

Tipos de informação	Seus valores
Endereços do servidor NTP Os endereços IP dos servidores NTP (Network Time Protocol) no seu site. Esses servidores são usados para sincronizar o tempo no cluster.	

Configure o ONTAP em um novo cluster com o Gerenciador do sistema

O System Manager fornece um fluxo de trabalho simples e fácil para configurar um novo cluster e configurar o armazenamento.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para utilizar o Gestor de sistema para configurar um cluster ONTAP. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Em alguns casos, como certas implantações do MetroCluster ou clusters que exigem endereçamento de rede IPv6, talvez seja necessário usar a CLI do ONTAP para configurar um novo cluster. Clique "aqui" para obter mais detalhes sobre esses requisitos, bem como as etapas para a configuração do cluster com a CLI do ONTAP.

Antes de começar

- Você deve ter instalado, cabeado e ligado o novo sistema de storage de acordo com as instruções de instalação e configuração do modelo da sua plataforma. Consulte "Documentação do AFF e do FAS" .
- As interfaces de rede do cluster devem ser configuradas em cada nó do cluster para comunicação intra-cluster.
- Você deve estar ciente dos seguintes requisitos de suporte do System Manager:
  - Quando você configura o gerenciamento de nós manualmente usando a CLI, o System Manager oferece suporte a apenas IPv4 GbE e não oferece suporte a IPv6 GbE. No entanto, se iniciar o System Manager após concluir a configuração de hardware utilizando DHCP com um endereço IP atribuído automaticamente e com a deteção do Windows, o System Manager pode configurar um endereço de gestão IPv6.

    No ONTAP 9.6 e versões anteriores, o Gerenciador de sistema não oferece suporte a implantações que exigem rede IPv6G.

  - O suporte à configuração do MetroCluster é para configurações IP do MetroCluster com dois nós em cada local.

    No ONTAP 9.7 e versões anteriores, o Gerenciador de sistema não oferece suporte à nova configuração de cluster para configurações do MetroCluster.

- Você deve reunir as seguintes informações:
  - Endereço IP de gerenciamento de cluster
  - Máscara de sub-rede da rede
  - Endereço IP do gateway de rede
  - Endereços IP do servidor DNS (Domain Name Services)
  - Endereços IP do servidor de Protocolo de tempo de rede

Atribua um endereço IP de gerenciamento de nó

Sistema Windows

Você deve conetar seu computador Windows à mesma sub-rede que os controladores. Isso atribuirá automaticamente um endereço IP de gerenciamento de nó ao seu sistema.

Passo

1. No sistema Windows, abra a unidade **Network** para descobrir os nós.
2. Clique duas vezes no nó para iniciar o assistente de configuração do cluster.

Outros sistemas

Você deve configurar o endereço IP de gerenciamento de nós para um dos nós do cluster. Você pode usar esse endereço IP de gerenciamento de nó para iniciar o assistente de configuração de cluster.

Consulte "Criando o cluster no primeiro nó" para obter informações sobre como atribuir um endereço IP de gerenciamento de nó.

Inicialize o cluster

Inicializar o cluster definindo uma senha administrativa para o cluster e configurando as redes de gerenciamento de cluster e de gerenciamento de nós. Você também pode configurar serviços como um servidor DNS para resolver nomes de host e um servidor NTP para sincronizar a hora.

Passos

1. Em um navegador da Web, insira o endereço IP de gerenciamento de nós que você configurou: "https://node-management-IP"

   O System Manager descobre automaticamente os nós restantes no cluster.

2. Em **Initialize storage system**, insira o nome do cluster e a senha de administrador.
3. Em **rede**, insira o endereço IP de gerenciamento de cluster, a máscara de sub-rede e o gateway.
4. Se você quiser usar o serviço de nome de domínio para resolver nomes de host, selecione **Use Domain Name Service (DNS)**; em seguida, insira as informações do servidor DNS.
5. Se pretender utilizar o NTP (Network Time Protocol) para manter os tempos sincronizados no cluster, em **outros**, selecione **utilizar serviços de tempo (NTP)** e, em seguida, introduza as informações do servidor NTP.
6. Clique em **Enviar**.

O que vem a seguir

Depois de inicializar o cluster, você pode "Execute o Active IQ Config Advisor para validar sua configuração e verificar se há erros de configuração comuns".

Crie seu nível local

Crie camadas locais a partir dos discos ou SSDs disponíveis em seus nós. O System Manager calcula automaticamente a melhor configuração de camada com base no seu hardware.

Passos

1. Clique em **Dashboard** e, em seguida, clique em **Prepare Storage**.

   Aceite a recomendação de storage do seu nível local.

Configurar protocolos

Dependendo das licenças ativadas no cluster, pode ativar os protocolos pretendidos no cluster. Em seguida, você cria interfaces de rede usando as quais você pode acessar o storage.

Passos

1. Clique em **Dashboard** e, em seguida, clique em **Configure Protocols**.
   - Ativar iSCSI ou FC para acesso SAN.

- Habilite NFS ou SMB para acesso nas.
- Habilite o NVMe para acesso FC-NVMe.

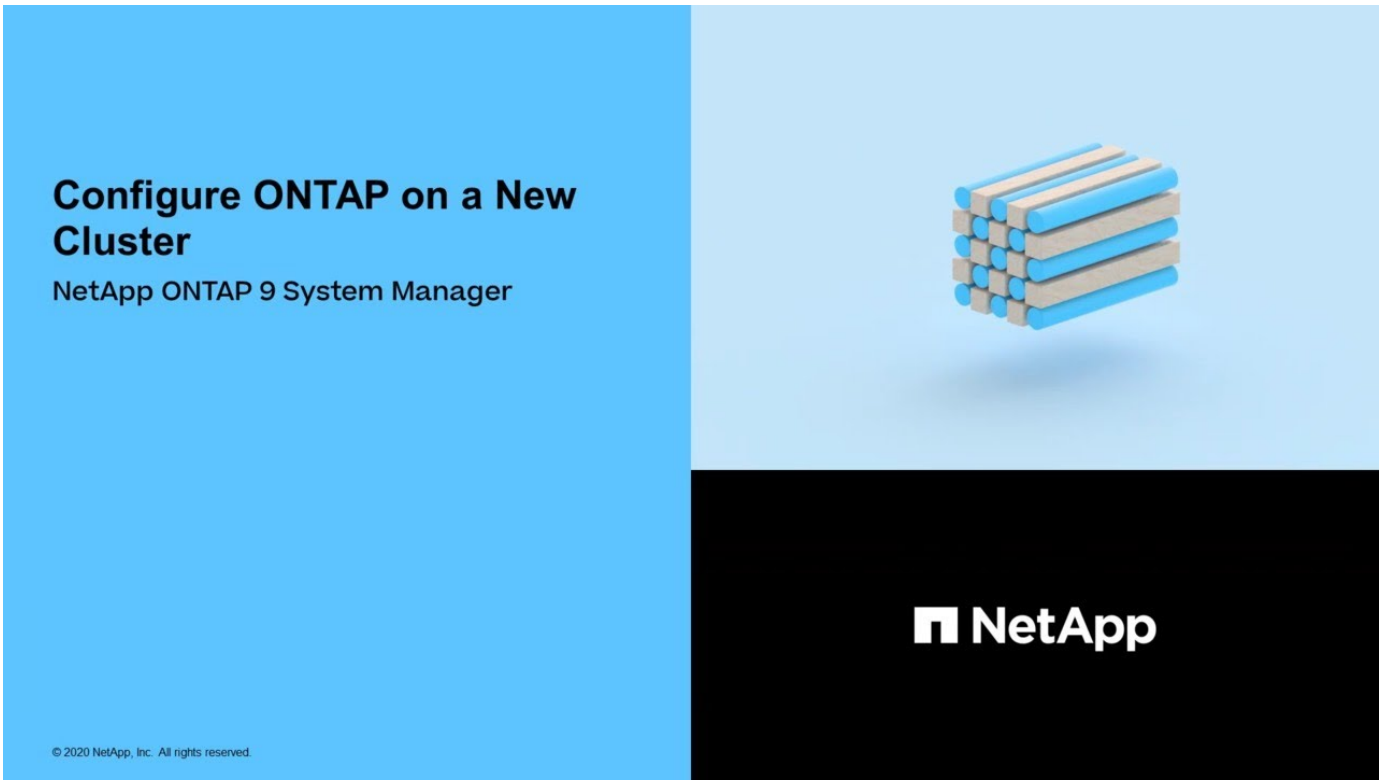
Provisionamento de storage

Depois de configurar protocolos, você pode provisionar o storage. As opções que você vê dependem das licenças que estão instaladas.

Passos

1. Clique em **Dashboard** e, em seguida, clique em **provision Storage**.
   - Para "Provisione acesso SAN", clique em **Add LUNs**.
   - Para "Provisionamento de acesso nas", clique em **Add volumes**.
   - Para "Provisionamento de storage NVMe", clique em **Add Namespaces**.

Configure o ONTAP em um novo vídeo de cluster



Configure um cluster com a CLI

Crie o cluster no primeiro nó

Você usa o assistente Configuração de cluster para criar o cluster no primeiro nó. O assistente ajuda você a configurar a rede de cluster que coneta os nós, criar a máquina virtual de armazenamento de administrador de cluster (SVM), adicionar chaves de licença de recurso e criar a interface de gerenciamento de nó para o primeiro nó.

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para utilizar o Gestor de sistema para configurar um cluster ONTAP. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Antes de começar

- Você deve ter instalado, cabeado e ligado o novo sistema de storage de acordo com as instruções de instalação e configuração do modelo da sua plataforma. Consulte "Documentação do AFF e do FAS" .
- As interfaces de rede do cluster devem ser configuradas em cada nó do cluster para comunicação intra-cluster.
- Se você estiver configurando o IPv6 em seu cluster, o IPv6 deve ser configurado no controlador de gerenciamento básico (BMC) para que você possa acessar o sistema usando SSH.

Passos

1. Ligue todos os nós que você está adicionando ao cluster. Isso é necessário para ativar o reconhecimento para a configuração do cluster.
2. Conete-se ao console do primeiro nó.

   O nó é inicializado e, em seguida, o assistente Configuração de cluster é iniciado no console.

   ```
   Welcome to the cluster setup wizard....
   ```

3. Confirme a declaração AutoSupport.

   ```
   Type yes to confirm and continue {yes}: yes
   ```

   O AutoSupport está ativado por predefinição.

4. Siga as instruções na tela para atribuir um endereço IP ao nó.

   A partir do ONTAP 9.13,1, você pode atribuir endereços IPv6 para LIFs de gerenciamento em plataformas A800 e FAS8700. Para versões do ONTAP anteriores a 9.13.1, ou para 9.13.1 e posteriores em outras plataformas, você deve atribuir endereços IPv4 para LIFs de gerenciamento e depois converter para IPv6 depois de concluir a configuração do cluster.

5. Pressione **Enter** para continuar.

   ```
   Do you want to create a new cluster or join an existing cluster?
   {create, join}:
   ```

6. Criar um novo cluster: `create`
7. Aceite as predefinições do sistema ou introduza os seus próprios valores.
8. Após a conclusão da configuração, faça login no cluster e verifique se o cluster está ativo e se o primeiro nó está em funcionamento, digitando o comando CLI do ONTAP: `cluster show`

O exemplo a seguir mostra um cluster no qual o primeiro nó (cluster1-01) está íntegro e qualificado para participar:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
```

Você pode acessar o assistente Configuração de cluster para alterar qualquer um dos valores inseridos para o SVM admin ou nó SVM usando o `cluster setup` comando.

Depois de terminar

Se necessário, "Converter de IPv4 para IPv6".

Junte os nós restantes ao cluster

Depois de criar um novo cluster, use o assistente Configuração de cluster para unir cada nó restante ao cluster um de cada vez. O assistente ajuda você a configurar a interface de gerenciamento de nó de cada nó.

> Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para utilizar o Gestor de sistema para configurar um cluster ONTAP. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Ao ingressar em dois nós em um cluster, você está criando um par de alta disponibilidade (HA). Se você juntar 4 nós, crie dois pares de HA. Para saber mais sobre HA, "Saiba mais sobre HA"consulte .

Você só pode unir um nó ao cluster de cada vez. Quando você começar a ingressar em um nó no cluster, deve concluir a operação de associação para esse nó e o nó deve fazer parte do cluster antes de começar a ingressar no próximo nó.

Prática recomendada: se você tiver um FAS2720 com 24 ou menos unidades NL-SAS, verifique se o padrão de configuração de armazenamento está definido como ativo/passivo para otimizar o desempenho. Para obter mais informações, consulte a documentação para "configurando uma configuração ativo-passivo em nós usando o particionamento de dados raiz".

1. Faça login no nó que você pretende ingressar no cluster.

   O assistente de configuração do cluster é iniciado no console.

   ```
   Welcome to the cluster setup wizard....
   ```

2. Confirme a declaração AutoSupport.

   > O AutoSupport está ativado por predefinição.

```
Type yes to confirm and continue {yes}: yes
```

3. Siga as instruções na tela para atribuir um endereço IP ao nó.

   A partir do ONTAP 9.13,1, você pode atribuir endereços IPv6 para LIFs de gerenciamento em plataformas A800 e FAS8700. Para versões do ONTAP anteriores a 9.13.1, ou para 9.13.1 e posteriores em outras plataformas, você deve atribuir endereços IPv4 para LIFs de gerenciamento e depois converter para IPv6 depois de concluir a configuração do cluster.

4. Pressione **Enter** para continuar.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

5. Junte o nó ao cluster: `join`
6. Siga as instruções na tela para configurar o nó e associá-lo ao cluster.
7. Após a conclusão da configuração, verifique se o nó está íntegro e qualificado para participar do cluster: `cluster show`

   O exemplo a seguir mostra um cluster após o segundo nó (cluster1-02) ter sido Unido ao cluster:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
cluster1-02           true    true
```

   Você pode acessar o assistente Configuração de cluster para alterar qualquer um dos valores inseridos para o SVM admin ou nó SVM usando o comando de configuração de cluster.

8. Repita esta tarefa para cada nó restante.

Depois de terminar

Se necessário, "Converter de IPv4 para IPv6".

Converter LIFs de gerenciamento de IPv4 para IPv6

A partir do ONTAP 9.13,1, você pode atribuir endereços IPv6 a LIFs de gerenciamento em plataformas A800 e FAS8700 durante a configuração inicial do cluster. Para versões do ONTAP anteriores a 9.13.1, ou para 9.13.1 e posteriores em outras plataformas, primeiro você deve atribuir endereços IPv4 a LIFs de gerenciamento e depois converter para endereços IPv6 depois de concluir a configuração do cluster.

Passos

1. Ativar IPv6 para o cluster:

```
network options ipv6 modify -enable true
```

2. Definir privilégio como avançado:

```
set priv advanced
```

3. Veja a lista de prefixos RA aprendidos em várias interfaces:

```
network ndp prefix show
```

4. Crie um LIF de gerenciamento IPv6:

   Use o formato `prefix::id` no parâmetro address para construir o endereço IPv6 manualmente.

```
network interface create -vserver <svm_name> -lif <LIF> -home-node
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask
-length <netmask_length> -failover-policy <policy> -service-policy
<service_policy> -auto-revert true
```

5. Verifique se o LIF foi criado:

```
network interface show
```

6. Verifique se o endereço IP configurado está acessível:

```
network ping6
```

7. Marque o IPv4 LIF como administrativamente para baixo:

```
network interface modify -vserver <svm_name> -lif <lif_name> -status
-admin down
```

8. Eliminar o LIF de gestão IPv4:

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. Confirme se o LIF de gerenciamento IPv4 é excluído:

```
network interface show
```

Verifique seu cluster com o Digital Advisor Config Advisor

Depois de associar todos os nós ao novo cluster, execute o Active IQ Config Advisor para validar a configuração e verificar se há erros comuns de configuração.

O Config Advisor é um aplicativo baseado na Web que você instala em seu laptop, máquina virtual ou servidor e funciona em plataformas Windows, Linux e Mac.

O Config Advisor executa uma série de comandos para validar a instalação e verificar a integridade geral da configuração, incluindo o cluster e os switches de armazenamento.

1. Baixe e instale o Active IQ Config Advisor.

   "Active IQ Config Advisor"

2. Inicie o Digital Advisor e configure uma frase-passe quando solicitado.
3. Revise suas configurações e clique em **Salvar**.
4. Na página **Objetivos**, clique em **Validação pós-implantação do ONTAP**.
5. Escolha o modo Guided ou Expert.

   Se escolher o modo guiado, os interrutores ligados são detetados automaticamente.

6. Insira as credenciais do cluster.
7. (Opcional) clique em **form validate**.
8. Para começar a coletar dados, clique em **Salvar e avaliar**.
9. Após a conclusão da coleta de dados, em **Monitor de trabalho > ações**, visualize os dados coletados clicando no ícone **Exibição de dados** e visualize os resultados clicando no ícone **resultados**.
10. Resolva os problemas identificados pelo Config Advisor.

Sincronize a hora do sistema no cluster

A sincronização do tempo garante que cada nó no cluster tenha o mesmo tempo e evita falhas CIFS e Kerberos.

Um servidor NTP (Network Time Protocol) deve ser configurado no seu site. A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica. Para obter mais informações, consulte a documentação para "gerenciamento do tempo do cluster (somente administradores de cluster)".

Você sincroniza a hora no cluster associando o cluster a um ou mais servidores NTP.

1. Verifique se a hora e o fuso horário do sistema estão definidos corretamente para cada nó.

   Todos os nós no cluster devem ser definidos para o mesmo fuso horário.

   a. Use o comando de exibição de data do cluster para exibir a data, hora e fuso horário atuais para cada nó.

```
cluster1::> cluster date show
Node         Date                Time zone
------------ ------------------- -----------------
cluster1-01  01/06/2015 09:35:15 America/New_York
cluster1-02  01/06/2015 09:35:15 America/New_York
cluster1-03  01/06/2015 09:35:15 America/New_York
cluster1-04  01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

b. Use o comando de modificação de data do cluster para alterar a data ou o fuso horário de todos os nós.

   Este exemplo altera o fuso horário do cluster para ser GMT:

```
cluster1::> cluster date modify -timezone GMT
```

2. Use o comando cluster time-service ntp Server Create para associar o cluster ao servidor ntp.

   - Para configurar seu servidor NTP sem autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_name`
   - Para configurar seu servidor NTP com autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id`

   > A autenticação simétrica está disponível a partir do ONTAP 9.5. Ele não está disponível no ONTAP 9.4 ou anterior.

   Este exemplo pressupõe que o DNS foi configurado para o cluster. Se não tiver configurado o DNS, tem de especificar o endereço IP do servidor NTP:

```
cluster1::> cluster time-service ntp server create -server
ntp1.example.com
```

3. Verifique se o cluster está associado a um servidor NTP: `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show
Server               Version
-------------------- -----------
ntp1.example.com     auto
```

Informações relacionadas

"Administração do sistema"

Comandos para gerenciar a autenticação simétrica em servidores NTP

A partir do ONTAP 9.5, o protocolo de tempo de rede (NTP) versão 3 é suportado. O NTPv3 inclui autenticação simétrica usando chaves SHA-1, o que aumenta a segurança da rede.

Para fazer isso…	Use este comando…
Configurar um servidor NTP sem autenticação simétrica	`cluster time-service ntp server create -server server_name`
Configure um servidor NTP com autenticação simétrica	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Ative a autenticação simétrica para um servidor NTP existente Um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID-chave necessário.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configurar uma chave NTP partilhada	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` **Nota:** as chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP
Configure um servidor NTP com um ID de chave desconhecido	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure um servidor com um ID de chave não configurado no servidor NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` **Nota:** o ID, tipo e valor da chave devem ser idênticos ao ID, tipo e valor da chave configurados no servidor NTP.
Desativar a autenticação simétrica	`cluster time-service ntp server modify -server server_name -authentication disabled`

Tarefas adicionais de configuração do sistema a serem concluídas

Depois de configurar um cluster, você pode usar o Gerenciador do sistema ou a interface de linha de comando (CLI) do ONTAP para continuar a configuração do cluster.

Tarefa de configuração do sistema	Recurso
Configurar rede: • Criar domínios de broadcast • Crie sub-redes • Crie espaços IP	"Configurar a rede"
Configure o processador de serviço	"Administração do sistema"
Coloque seus agregados	"Gerenciamento de disco e agregado"
Criar e configurar máquinas virtuais de armazenamento de dados (SVMs)	"Configuração NFS" "Configuração SMB" "Administração da SAN"
Configurar notificações de eventos	"Configuração EMS"

Configurar o software All-Flash SAN Array

Visão geral da configuração do software All-Flash SAN Array

Os ASAs (All-Flash SAN Arrays) da NetApp estão disponíveis a partir do ONTAP 9.7. Os asas são soluções all-flash somente SAN criadas em plataformas AFF NetApp comprovadas.

A partir do ONTAP 9.16,0, uma experiência de ONTAP simplificada específica para clientes somente SAN está disponível nos sistemas ASA R2 (ASA A1K, ASA A70 ou ASA A90). Se tiver um sistema ASA R2, consulte "Documentação do sistema ASA R2".

As plataformas ASA usam ativo-ativo simétrico para multipathing. Todos os caminhos estão ativos/otimizados, portanto, no caso de um failover de storage, o host não precisa esperar pela transição do ALUA dos caminhos de failover para retomar a I/O. Isso reduz o tempo de failover.

Configure um ASA

Os All-Flash SAN Arrays (ASAs) seguem o mesmo procedimento de configuração que os sistemas que não são ASA.

O System Manager orienta você pelos procedimentos necessários para inicializar o cluster, criar um nível local, configurar protocolos e provisionar storage para o ASA.

Comece a configurar o cluster do ONTAP.

Configurações e utilitários do host do ASA

As configurações de host para a configuração de all-flash SAN Arrays (ASAs) são as mesmas de todos os outros hosts SAN.

Você pode baixar o "Software de utilitários de host NetApp" para seus hosts específicos a partir do site de suporte.

Maneiras de identificar um sistema ASA

Você pode identificar um sistema ASA usando o Gerenciador do sistema ou usando a interface de linha de comando (CLI) do ONTAP.

- **No painel do System Manager**: Clique em **Cluster > Overview** e selecione o nó do sistema.

  O **PERSONALITY** é exibido como **All-Flash SAN Array**.

- **Da CLI**: Digite o `san config show` comando.

  O valor "array all-flash SAN" retorna como verdadeiro para sistemas ASA.

Informações relacionadas

- "Relatório técnico 4968: Integridade e disponibilidade dos dados de array all-SAN da NetApp"
- "Relatório técnico da NetApp 4080: Práticas recomendadas para SAN moderna"

Limites de configuração e suporte do All-Flash SAN Array

Os limites de configuração e suporte do All-Flash SAN Array (ASA) variam de acordo com a versão do ONTAP.

Os detalhes mais atuais sobre os limites de configuração suportados estão disponíveis no "NetApp Hardware Universe".

> Essas limitações se aplicam aos sistemas ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), "Limites de storage do sistema ASA R2"consulte .

Protocolos SAN e número de nós com suporte por cluster

Os protocolos SAN compatíveis e o número máximo de nós por cluster dependem de você ter uma configuração que não seja MetroCluster ou MetroCluster:

Configurações que não são MetroCluster

A tabela a seguir mostra o suporte do ASA para protocolos SAN e o número de nós suportados por cluster em configurações que não sejam MetroCluster:

Começando com ONTAP…	Suporte ao protocolo	Máximo de nós por cluster
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • ISCSI	12
9,7	• FC • ISCSI	2

Configurações IP do MetroCluster

A tabela a seguir mostra o suporte do ASA para protocolos SAN e o número de nós suportados por cluster nas configurações IP do MetroCluster:

Começando com ONTAP…	Suporte ao protocolo	Máximo de nós por cluster
9.15.1	• NVMe/TCP	2 nós por cluster em configurações de IP MetroCluster de quatro nós
9.12.1	• NVMe/FC	2 nós por cluster em configurações de IP MetroCluster de quatro nós
9.9.1	• FC • ISCSI	4 nós por cluster em configurações de IP MetroCluster de oito nós
9,7	• FC • ISCSI	2 nós por cluster em configurações de IP MetroCluster de quatro nós

Suporte para portas persistentes

A partir do ONTAP 9.8, as portas persistentes são habilitadas por padrão em all-flash SAN Arrays (asas all-flash) configurados para usar o protocolo FC. As portas persistentes estão disponíveis apenas para FC e exigem associação de zona identificada pelo World Wide Port Name (WWPN).

As portas persistentes reduzem o impactos das aquisições criando um LIF de sombra na porta física correspondente do parceiro de alta disponibilidade (HA). Quando um nó é assumido, o LIF sombra no nó parceiro assume a identidade do LIF original, incluindo o WWPNe. Antes que o status do caminho para o nó tomado sobre seja alterado para defeituoso, o Shadow LIF aparece como um caminho ativo/otimizado para a pilha MPIO do host, e I/o é deslocado. Isso reduz a interrupção de e/S porque o host sempre vê o mesmo número de caminhos para o destino, mesmo durante operações de failover de storage.

Para portas persistentes, as seguintes características de porta FCP devem ser idênticas no par de HA:

- Contagens de portas FCP
- Nomes de portas FCP
- Velocidades de porta FCP
- Zoneamento baseado em WWPN do FCP

Se alguma destas caraterísticas não for idêntica no par HA, é gerada a seguinte mensagem EMS:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Para obter mais informações sobre portas persistentes, "Relatório técnico da NetApp 4080: Práticas recomendadas para SAN moderna"consulte .

Atualize ONTAP

Visão geral da atualização do ONTAP

Ao atualizar seu software ONTAP, você pode aproveitar os novos e aprimorados recursos do ONTAP que ajudam a reduzir custos, acelerar workloads críticos, melhorar a segurança e expandir o escopo de proteção de dados disponível para sua organização.

Uma grande atualização do ONTAP consiste em passar de uma versão menor para maior número de ONTAP. Um exemplo seria uma atualização do cluster do ONTAP 9.8 para o ONTAP 9.12,1. Uma atualização menor (ou patch) consiste em passar de uma versão mais baixa do ONTAP para uma versão mais alta do ONTAP dentro da mesma versão numerada. Um exemplo seria uma atualização do cluster de ONTAP 9.12.1P1 para 9.12.1P4.

Para começar, você deve se preparar para a atualização. Se você tiver um contrato SupportEdge ativo para o consultor digital da Active IQ (também conhecido como consultor digital), você deve "Prepare-se para atualizar com o Upgrade Advisor". O Upgrade Advisor fornece inteligência que ajuda você a minimizar a incerteza e o risco, avaliando seu cluster e criando um plano de atualização específico para sua configuração. Se você não tiver um contrato SupportEdge ativo para o consultor digital da Active IQ, você deve "Prepare-se para atualizar sem o Upgrade Advisor".

Depois de se preparar para a atualização, é recomendável que você execute atualizações usando "Atualização automatizada e sem interrupções (ANDU) do System Manager"o . O ANDU aproveita a tecnologia de failover de alta disponibilidade (HA) da ONTAP para garantir que os clusters continuem fornecendo dados sem interrupção durante a atualização.

> A partir do ONTAP 9.12,1, o Gerenciador de sistema é totalmente integrado ao BlueXP . Se o BlueXP estiver configurado no seu sistema, você poderá fazer upgrade pelo ambiente de trabalho do BlueXP .

Se você quiser obter assistência para atualizar seu software ONTAP, os Serviços profissionais da NetApp oferecem um "Serviço de atualização gerenciada". Se estiver interessado em utilizar este serviço, contacte o seu representante de vendas da NetApp ou "Envie o formulário de inquérito de vendas da NetApp". O Serviço de Atualização gerenciada, bem como outros tipos de suporte de atualização, estão disponíveis para clientes "Serviços da SupportEdge Expert"sem nenhum custo adicional.

Quando devo atualizar o ONTAP?

Você deve atualizar seu software ONTAP em uma cadência regular. Atualizar o ONTAP permite que você aproveite os recursos e funcionalidades novos e aprimorados e implemente correções atuais para problemas conhecidos.

Principais atualizações do ONTAP

Uma grande atualização do ONTAP ou lançamento de recursos normalmente inclui:

- Novos recursos do ONTAP
- Principais alterações na infraestrutura, como alterações fundamentais na operação NetApp WAFL ou operação RAID
- Suporte para novos sistemas de hardware projetados pela NetApp
- Suporte para componentes de hardware de substituição, como placas de interface de rede mais recentes ou adaptadores de barramento de host

Os novos lançamentos do ONTAP têm direito a suporte total por 3 anos. A NetApp recomenda que você execute a versão mais recente por 1 ano após a disponibilidade geral (GA) e, em seguida, use o tempo restante dentro da janela de suporte completa para Planejar sua transição para uma versão mais recente do ONTAP.

Atualizações de patch do ONTAP

As atualizações de patches oferecem correções oportunas para bugs críticos que não podem esperar pela próxima versão principal do recurso ONTAP. Atualizações de patch não críticas devem ser aplicadas a cada 3-6 meses. Atualizações críticas de patches devem ser aplicadas o mais rápido possível.

Saiba mais sobre "níveis mínimos de patch recomendados" os lançamentos do ONTAP.

Datas de lançamento do ONTAP

Começando com o lançamento do ONTAP 9.8, o NetApp entrega lançamentos do ONTAP duas vezes por ano civil. Embora os planos estejam sujeitos a mudanças, a intenção é entregar novos lançamentos do ONTAP no segundo e quarto trimestre de cada ano civil. Use essas informações para Planejar o período de tempo da atualização para aproveitar a versão mais recente do ONTAP.

Versão	Data de lançamento
9.16.1	Novembro de 2024
9.15.1	Maio de 2024
9.14.1	Janeiro de 2024

Versão	Data de lançamento
9.13.1	Junho de 2023
9.12.1	Fevereiro de 2023
9.11.1	Julho de 2022
9.10.1	Janeiro de 2022
9.9.1	Junho de 2021

Níveis de suporte da ONTAP

O nível de suporte disponível para uma versão específica do ONTAP varia dependendo de quando o software foi lançado.

Nível de suporte	Suporte completo			Suporte limitado		Suporte por autoatendimento		
Ano	1	2	3	4	5	6	7	8
Acesso à documentação online	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Suporte técnico	Sim	Sim	Sim	Sim	Sim			
Análise de causa raiz	Sim	Sim	Sim	Sim	Sim			
Downloads de software	Sim	Sim	Sim	Sim	Sim			
Atualizações de serviço (versões de patch [P-lançamentos])	Sim	Sim	Sim					
Alertas sobre vulnerabilidades	Sim	Sim	Sim					

Informações relacionadas

- "Novidades nas versões ONTAP atualmente suportadas"Aprenda .
- Saiba mais "Mínimo recomendado de lançamentos de ONTAP"sobre o .
- Saiba mais "Suporte à versão do software ONTAP"sobre o .
- Saiba mais sobre o "Modelo de lançamento do ONTAP".

Execute verificações de pré-atualização automatizadas do ONTAP antes de uma atualização planejada

Você não precisa estar no processo de atualização do seu software ONTAP para executar as pré-verificações de atualização automatizada ONTAP. Executar as verificações de pré-atualização independentemente do processo de atualização automatizada do ONTAP permite que você veja quais verificações são executadas em seu cluster e fornece uma lista de quaisquer erros ou avisos que devem ser corrigidos antes de iniciar a atualização real. Por exemplo, suponha que você espera atualizar seu software ONTAP durante uma janela de manutenção programada para ocorrer em duas semanas. Enquanto aguarda a data agendada, pode executar as pré-verificações automáticas de atualização e efetuar quaisquer ações corretivas necessárias antes da janela de manutenção. Isso irá mitigar os riscos de erros de configuração inesperados depois de iniciar a atualização.

Se estiver pronto para iniciar a atualização do software ONTAP, não é necessário executar este procedimento. Você deve seguir o "processo de atualização automatizado", que inclui a execução das pré-verificações de atualização automatizada.

> Para configurações do MetroCluster, você deve primeiro executar estas etapas no cluster A e, em seguida, executar as mesmas etapas no cluster B.

Antes de começar

Você deve "Transfira a imagem do software ONTAP de destino".

Para executar as pré-verificações de atualização automatizada para um "atualização direta de multi-hop", você só precisa fazer o download do pacote de software para a versão ONTAP de destino. Você não precisará carregar a versão intermediária do ONTAP até começar a atualização real. Por exemplo, se você estiver executando verificações automatizadas de pré-atualização para uma atualização de 9,7 para 9.11.1, você precisará baixar o pacote de software para o ONTAP 9.11,1. Você não precisa baixar o pacote de software para ONTAP 9.8,1.

Exemplo 1. Passos

System Manager

1. Valide a imagem de destino ONTAP:

   Se você estiver atualizando uma configuração do MetroCluster, valide o cluster A e repita o processo de validação no cluster B.

   a. Dependendo da versão do ONTAP que você está executando, execute uma das seguintes etapas:

Se você está correndo…	Faça isso…
ONTAP 9 .8 ou posterior	Clique em **Cluster > Overview**.
ONTAP 9.5, 9,6 e 9,7	Clique em **Configuração** > **Cluster** > **Atualizar**.
ONTAP 9 .4 ou anterior	Clique em **Configuração** > **Atualização de cluster**.

   b. No canto direito do painel **Visão geral**, clique em .

   c. Clique em **Atualização do ONTAP**.

   d. Na guia **Atualização de cluster**, adicione uma nova imagem ou selecione uma imagem disponível.

Se você quiser…	Então…
Adicione uma nova imagem de software a partir de uma pasta local Você já deve ter "transferir a imagem"para o cliente local.	i. Em **imagens de software disponíveis**, clique em **Adicionar do local**. ii. Navegue até o local onde você salvou a imagem do software, selecione a imagem e clique em **Open**.
Adicione uma nova imagem de software a partir de um servidor HTTP ou FTP	i. Clique em **Adicionar do servidor**. ii. Na caixa de diálogo **Adicionar uma nova imagem de software**, insira o URL do servidor HTTP ou FTP para o qual você baixou a imagem do software ONTAP do site de suporte da NetApp. Para FTP anônimo, você deve especificar a URL no ftp://anonymous@ftpserver formato. iii. Clique em **Add**.
Selecione uma imagem disponível	Escolha uma das imagens listadas.

e. Clique em **Validar** para executar as verificações de validação de pré-atualização.

   Se forem encontrados erros ou avisos durante a validação, estes são apresentados juntamente com uma lista de acões correctivas. Você deve resolver todos os erros antes de prosseguir com a atualização. É prática recomendada também resolver avisos.

CLI

1. Carregue a imagem de software ONTAP de destino no repositório de pacotes do cluster:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.15.1/image.tgz

Package download completed.
Package processing completed.
```

2. Verifique se o pacote de software está disponível no repositório de pacotes de cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.15.1             MM/DD/YYYY 10:32:15
```

3. Execute as verificações automatizadas de pré-atualização:

```
cluster image validate -version <package_version_number> -show
-validation-details true
```

```
cluster1::> cluster image validate -version 9.15.1 -show-validation
-details true

It can take several minutes to complete validation...
Validation checks started successfully.  Run the "cluster image
show-update-progress" command to check validation status.
```

4. Verificar o estado de validação:

```
cluster image show-update-progress
```

Se o **Status** estiver "em andamento", aguarde e execute o comando novamente até que ele esteja concluído.

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                    Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                 00:10:00
00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
...
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

É apresentada uma lista de pré-verificações automáticas completas de atualização, juntamente com quaisquer erros ou avisos que devem ser resolvidos antes de iniciar o processo de atualização.

Exemplo de saída

Exemplo completo de saída de pré-verificações de atualização

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to
be performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Use the Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system
supportability configuration information.

Validation checks started successfully.  Run the "cluster image show-
update-progress" command to check validation status.


fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    in-progress            00:10:00        00:00:42

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
---------------------------------------

fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    completed              00:10:00        00:01:03
```

```
Details:

Pre-update Check     Status            Error-Action
-------------------- ----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
Configuration Status
Boot Menu Status     Warning           Warning: bootarg.init.bootmenu
is
                                       enabled on nodes: fas2820-wic-
1a,
                                       fas2820-wic-1b. The boot process
of
                                       the nodes will be delayed.
                                       Action: Set the
bootarg.init.bootmenu
                                       bootarg to false before
proceeding
                                       with the upgrade.
Broadcast Domain     OK                N/A
availability and
uniqueness for HA
pair status
CIFS compatibility   OK                N/A
status check
CLAM quorum online   OK                N/A
status check
CPU Utilization      OK                N/A
Status
Capacity licenses    OK                N/A
install status check
Check For SP/BMC     OK                N/A
Connectivity To
Nodes
```

```
Check LDAP fastbind  OK              N/A
users using
unsecure connection.
Check for unsecure   OK              N/A
kex algorithm
configurations.
Check for unsecure   OK              N/A
mac configurations.
Cloud keymanager     OK              N/A
connectivity check
Cluster health and   OK              N/A
eligibility status
Cluster quorum       OK              N/A
status check
Cluster/management   OK              N/A
switch check
Compatible New       OK              N/A
Image Check
Current system       OK              N/A
version check if it
is susceptible to
possible outage
during NDU
Data ONTAP Version   OK              N/A
and Previous
Upgrade Status
Data aggregates HA   OK              N/A
policy check
Disk status check    OK              N/A
for failed, broken
or non-compatibility
Duplicate Initiator  OK              N/A
Check
Encryption key       OK              N/A
migration status
check
External             OK              N/A
key-manager with
legacy KMIP client
check
External keymanager  OK              N/A
key server status
check
Fabricpool Object    OK              N/A
Store Availability
High Availability    OK              N/A
```

```
configuration
status check
Infinite Volume      OK               N/A
availibility check
LIF failover         OK               N/A
capability status
check
LIF health check     OK               N/A
LIF load balancing   OK               N/A
status check
LIFs is on home      OK               N/A
node status
Logically over       OK               N/A
allocated DP
volumes check
MetroCluster         OK               N/A
configuration
status check for
compatibility
Minimum number of    OK               N/A
aggregate disks
check
NAE Aggregate and    OK               N/A
NVE Volume
Encryption Check
NDMP sessions check  OK               N/A
NFS mounts status    Warning          Warning: This cluster is serving
NFS
check                                 clients. If NFS soft mounts are
used,
                                      there is a possibility of
frequent
                                      NFS timeouts and race conditions
that
                                      can lead to data corruption
during
                                      the upgrade.
                                      Action: Use NFS hard mounts, if
                                      possible. To list Vservers
running
                                      NFS, run the following command:
                                      vserver nfs show
Name Service         OK               N/A
Configuration DNS
Check
Name Service         OK               N/A
```

```
Configuration LDAP
Check
Node to SP/BMC       OK                N/A
connectivity check
OKM/KMIP enabled     OK                N/A
systems - Missing
keys check
ONTAP API to REST    Warning           Warning: NetApp ONTAP API has
been
transition warning                     used on this cluster for ONTAP
data
                                       storage management within the
last 30
                                       days. NetApp ONTAP API is
approaching
                                       end of availability.
                                       Action: Transition your
automation
                                       tools from ONTAP API to ONTAP
REST
                                       API. For more details, refer to
                                       CPC-00410 - End of availability:
                                       ONTAPI

https://mysupport.netapp.com/info/
                                       communications/ECMLP2880232.html
ONTAP Image          OK                N/A
Capability Status
OpenSSL 3.0.x        OK                N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                N/A
validation check
Platform Health      OK                N/A
Monitor check
Pre-Update           OK                N/A
Configuration
Verification
RDB Replica Health   OK                N/A
Check
Replicated database  OK                N/A
schema consistency
check
Running Jobs Status  OK                N/A
SAN LIF association  OK                N/A
status check
```

```
SAN compatibility    OK                N/A
for manual
configurability
check
SAN kernel agent     OK                N/A
status check
Secure Purge         OK                N/A
operation Check
Shelves and Sensors  OK                N/A
check
SnapLock Version     OK                N/A
Check
SnapMirror           OK                N/A
Synchronous
relationship status
check
SnapMirror           OK                N/A
compatibility
status check
Supported platform   OK                N/A
check
Target ONTAP         OK                N/A
release support for
FiberBridge 6500N
check
Upgrade Version      OK                N/A
Compatibility Status
Verify all bgp       OK                N/A
peer-groups are in
the up state
Verify if a cluster  OK                N/A
management LIF
exists
Verify that e0M is   OK                N/A
home to no LIFs
with high speed
services.
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
```

```
Overall Status       Warning           Warning
75 entries were displayed.
```

Prepare-se para uma atualização do ONTAP

Determine quanto tempo uma atualização do ONTAP levará

Você deve Planejar por pelo menos 30 minutos para concluir as etapas preparatórias para uma atualização do ONTAP, 60 minutos para atualizar cada par de HA e pelo menos 30 minutos para concluir as etapas pós-atualização.

> Se você estiver usando a criptografia NetApp com um servidor de gerenciamento de chaves externo e o KMIP (Key Management Interoperability Protocol), espere que a atualização para cada par de HA seja maior que uma hora.

Essas diretrizes de duração de atualização são baseadas em configurações e workloads típicos. Use essas diretrizes para estimar o tempo necessário para realizar uma atualização sem interrupções no ambiente. A duração real do seu processo de atualização dependerá do seu ambiente individual e do número de nós.

Planeje sua atualização do ONTAP com o Supervisor de Atualização

Se você tiver um contrato ativo "Serviços da SupportEdge"para "Consultor digital"o , é recomendável usar o Upgrade Advisor para gerar um plano de atualização.

O serviço Upgrade Advisor no Digital Advisor fornece inteligência que ajuda você a Planejar sua atualização e minimiza a incerteza e o risco.

O Digital Advisor identifica problemas no seu ambiente que podem ser resolvidos atualizando para uma versão mais recente do ONTAP. O serviço de recomendações de atualização ajuda você a Planejar uma atualização bem-sucedida e fornece um relatório de problemas que você pode precisar estar ciente na versão do ONTAP para a qual você está atualizando.

> O Supervisor de Atualização requer um pacote AutoSupport completo para criar o relatório.

Se você não tiver um contrato de serviços de borda de suporte ativo para o Digital Advisor, deverá "Prepare-se para o seu upgrade sem o Upgrade Advisor".

Passos

1. "Inicie o consultor digital da Active IQ"
2. No Digital Advisor "visualize todos os riscos associados ao cluster e tome medidas corretivas manualmente".

   Os riscos incluídos nas categorias **alteração de configuração de software**, **alteração de configuração de hardware** e **Substituição de hardware** precisam ser resolvidos antes de realizar uma atualização do ONTAP.

3. Reveja o caminho de atualização recomendado e "gere o seu plano de atualização".

O que vem a seguir

- Você deve analisar a "Notas de versão do ONTAP"versão de destino do ONTAP recomendada para o cluster pelo Supervisor de Atualização; em seguida, você deve seguir o plano gerado pelo Consultor de Atualização para atualizar o cluster.
- Você deve "Reinicie o SP ou o BMC" antes do início da atualização.

Informações relacionadas

- "Como fazer upload manual de mensagens do AutoSupport para o NetApp"

Prepare-se para atualizar sem o Upgrade Advisor

Prepare-se para uma atualização do software ONTAP sem o consultor de atualização

A preparação adequada para uma atualização de software do ONTAP ajuda a identificar e mitigar possíveis riscos de atualização ou bloqueadores antes de iniciar o processo de atualização. Durante a preparação da atualização, você também pode identificar quaisquer considerações especiais que você possa precisar considerar antes de atualizar. Por exemplo, se o modo SSL FIPS estiver ativado no cluster e as contas de administrador usarem chaves públicas SSH para autenticação, você precisará verificar se o algoritmo da chave do host é suportado na versão do ONTAP de destino.

Se tiver um contrato SupportEdge ativo para "Consultor digital", "Planeje sua atualização com o Upgrade Advisor". Se você não tiver acesso ao consultor digital do Active IQ (também conhecido como consultor digital), faça o seguinte para se preparar para uma atualização do ONTAP.

1. "Escolha o seu lançamento de ONTAP de destino".
2. Reveja "Notas de versão do ONTAP"a para obter a versão alvo.

   A seção "Avisos de atualização" descreve possíveis problemas que você deve estar ciente antes de atualizar para a nova versão. As seções "o que há de novo" e "problemas e limitações conhecidos" descrevem o novo comportamento do sistema após a atualização para a nova versão.

3. "Confirme o suporte do ONTAP para sua configuração de hardware".

   Sua plataforma de hardware, switches de gerenciamento de cluster e switches IP MetroCluster devem oferecer suporte ao lançamento de destino. Se o cluster estiver configurado para SAN, a configuração da SAN deve ser totalmente suportada.

4. "Use o Active IQ Config Advisor para verificar se você não tem erros de configuração comuns."
5. Revise o ONTAP suportado "caminhos de atualização"para determinar se você pode realizar uma atualização direta ou se precisa concluir a atualização por etapas.
6. "Verifique a configuração de failover de LIF".

   Antes de realizar uma atualização, é necessário verificar se as políticas de failover e os grupos de failover do cluster estão configurados corretamente.

7. "Verifique a configuração de roteamento SVM".
8. "Verifique considerações especiais" para o cluster.

   Se houver certas configurações no cluster, há ações específicas que você precisa executar antes de iniciar uma atualização de software do ONTAP.

9. "Reinicie o SP ou o BMC".

Escolha a versão de destino do ONTAP para uma atualização

Quando você usa o Supervisor de Atualização para gerar um plano de atualização para o cluster, o plano inclui uma versão recomendada do ONTAP de destino para atualização. A recomendação fornecida pelo Supervisor de Atualização baseia-se na configuração atual e na versão atual do ONTAP.

Se você não usar o Supervisor de Atualização para Planejar sua atualização, escolha a versão de destino do ONTAP para a atualização com base nas recomendações do NetApp ou na versão mínima para atender às necessidades de desempenho do .

- Atualize para a versão mais recente disponível (recomendado)

  A NetApp recomenda que você atualize seu software ONTAP para a versão de patch mais recente da versão de ONTAP numerada mais recente. Se isso não for possível porque a versão numerada mais recente não é suportada pelos sistemas de armazenamento no cluster, você deve atualizar para a versão numerada mais recente suportada.

- Versão mínima recomendada

  Se você quiser restringir sua atualização à versão mínima recomendada para o cluster, consulte "Mínimo recomendado de lançamentos de ONTAP" para determinar a versão do ONTAP para a qual você deve atualizar.

Confirme o suporte do ONTAP para sua configuração de hardware

Antes de atualizar o ONTAP, você deve confirmar se a configuração de hardware pode suportar a versão de destino do ONTAP.

Todas as configurações

Use "NetApp Hardware Universe" para confirmar se a plataforma de hardware e os switches de cluster e gerenciamento são suportados na versão de destino do ONTAP.

A versão do ONTAP para a qual você pode atualizar pode ser limitada com base na configuração do hardware. Se o seu hardware não suportar a versão do software ONTAP para a qual pretende atualizar, terá de adicionar primeiro novos nós ao cluster, migrar os dados, remover os nós mais antigos e, em seguida, atualizar o software ONTAP. Siga o procedimento para "Adicionar novos nós a um cluster do ONTAP".

Os switches de cluster e gerenciamento incluem os switches de rede de cluster (NX-os), os switches de rede de gerenciamento (IOS) e o arquivo de configuração de referência (RCF). Se o cluster e os switches de gerenciamento forem suportados, mas não estiverem executando as versões mínimas de software necessárias para a versão de destino do ONTAP, atualize seus switches para versões de software compatíveis.

- "Downloads do NetApp: Switches de cluster Broadcom"
- "Downloads do NetApp: Switches Ethernet Cisco"
- "Downloads do NetApp: Switches de cluster do NetApp"

Se você precisar atualizar seus switches, a NetApp recomenda que você conclua primeiro a atualização do software ONTAP e, em seguida, execute a atualização de software para seus switches.

Configurações do MetroCluster

Antes de atualizar o ONTAP, se você tiver uma configuração do MetroCluster, use o "Ferramenta de Matriz de interoperabilidade do NetApp" para confirmar que seus switches IP do MetroCluster são suportados na versão do ONTAP de destino.

Configurações de SAN

Antes de atualizar o ONTAP, se o cluster estiver configurado para SAN, use o "Ferramenta de Matriz de interoperabilidade do NetApp" para confirmar se a configuração da SAN é totalmente compatível.

Todos os componentes SAN, incluindo a versão de software ONTAP de destino, o sistema operacional do host e patches, o software de utilitários de host necessários, o software de multipathing e os drivers e firmware do adaptador, devem ser suportados.

Identificar erros de configuração com o Active IQ Config Advisor

Antes de atualizar o ONTAP, você pode usar a ferramenta Active IQ Config Advisor para verificar se há erros de configuração comuns.

O Active IQ Config Advisor é uma ferramenta de validação de configuração para sistemas NetApp. Ele pode ser implantado em locais seguros e não seguros para coleta de dados e análise do sistema.

O suporte para Active IQ Config Advisor é limitado e está disponível apenas online.

Passos

1. Inicie sessão no "Site de suporte da NetApp"e, em seguida, clique em **Tools** > **Tools**.
2. Em **Active IQ Config Advisor**, clique "Transfira a aplicação"em .
3. Baixe, instale e execute o Active IQ Config Advisor.
4. Depois de executar o Active IQ Config Advisor, revise a saída da ferramenta e siga as recomendações fornecidas para resolver quaisquer problemas descobertos pela ferramenta.

Caminhos de atualização do ONTAP compatíveis

A versão do ONTAP para a qual você pode atualizar depende da plataforma de hardware e da versão do ONTAP atualmente em execução nos nós do cluster.

Para verificar se a plataforma de hardware é suportada para a versão de atualização de destino, "NetApp Hardware Universe" consulte . Utilize os "Ferramenta de Matriz de interoperabilidade do NetApp" "confirme o suporte para sua configuração"para .

Para determinar sua versão atual do ONTAP:

- No System Manager, clique em **Cluster > Overview**.
- A partir da interface de linha de comando (CLI), use o `cluster image show` comando. Você também pode usar o `system node image show` comando no nível de privilégio avançado para exibir detalhes.

Tipos de caminhos de atualização

Sempre que possível, são recomendadas atualizações automatizadas sem interrupções (ANDU). Dependendo de suas versões atuais e de destino, seu caminho de upgrade será **Direct**, **Direct multi-hop** ou **multi-stage**.

- **Direct**

  Você sempre pode atualizar diretamente para a próxima família de versões adjacentes do ONTAP usando uma única imagem de software. Para muitas versões, você também pode instalar uma imagem de software que permite atualizar diretamente para versões que são até quatro versões posteriores à versão em execução.

  Por exemplo, você pode usar o caminho de atualização direta de 9.11.1 para 9.12.1, ou de 9.11.1 para 9.15.1.

  Todos os caminhos de atualização *Direct* são suportados para "clusters de versões mistas".

- * Multi-hop direto *

  Para algumas atualizações automatizadas sem interrupções (ANDU) para versões não adjacentes, você precisa instalar a imagem de software para uma versão intermediária, bem como a versão de destino. O processo de atualização automatizada usa a imagem intermediária em segundo plano para concluir a atualização para a versão de destino.

  Por exemplo, se o cluster estiver executando 9,3 e você quiser atualizar para 9,7, você carregaria os pacotes de instalação do ONTAP para 9,5 e 9,7, em seguida, iniciaria ANDU para 9,7. O ONTAP atualiza automaticamente o cluster primeiro para 9,5 e depois para 9,7. Você deve esperar várias operações de aquisição/giveback e reinicializações relacionadas durante o processo.

- * Multi-stage *

  Se um caminho de multi-hop direto ou direto não estiver disponível para sua versão de destino não adjacente, você deve primeiro atualizar para uma versão intermediária suportada e, em seguida, atualizar para a versão de destino.

  Por exemplo, se você estiver executando o 9,6 e quiser atualizar para o 9.11.1, você deve concluir uma atualização de vários estágios: Primeiro de 9,6 para 9,8 e depois de 9,8 para 9.11.1. Atualizações de versões anteriores podem exigir três ou mais estágios, com várias atualizações intermediárias.

  > Antes de iniciar atualizações em vários estágios, certifique-se de que a versão de destino seja suportada na plataforma de hardware.

Antes de iniciar qualquer atualização importante, é uma prática recomendada atualizar primeiro para a versão de patch mais recente da versão do ONTAP em execução no cluster. Isso garantirá que quaisquer problemas na versão atual do ONTAP sejam resolvidos antes da atualização.

Por exemplo, se o seu sistema estiver executando o ONTAP 9.3P9 e você estiver planejando atualizar para o 9.11.1, você deve primeiro atualizar para a versão mais recente do patch 9,3 e seguir o caminho de atualização de 9,3 para 9.11.1.

Saiba mais "Mínimo recomendado de lançamentos de ONTAP no site de suporte da NetApp"sobre .

Caminhos de atualização suportados

Os seguintes caminhos de atualização são suportados para atualizações automáticas e manuais do seu software ONTAP. Esses caminhos de atualização se aplicam ao ONTAP e ao ONTAP Select no local. Existem diferentes "Caminhos de atualização compatíveis para o Cloud Volumes ONTAP".

Para clusters ONTAP de versão mista: Todos os caminhos de atualização *direct* e *direct multi-hop* incluem versões ONTAP compatíveis com clusters de versão mista. As versões do ONTAP incluídas em atualizações *multi-estágio* não são compatíveis para clusters de versões mistas. Por exemplo, uma atualização de 9,8 para 9.12.1 é uma atualização *direct*. Um cluster com nós executando 9,8 e 9.12.1 é um cluster de versão mista compatível. Uma atualização de 9,8 para 9.13.1 é uma atualização *multi-stage*. Um cluster com nós executando 9,8 e 9.13.1 não é um cluster de versão mista compatível.

A partir de ONTAP 9.10,1 e posterior

As atualizações automatizadas e manuais do ONTAP 9.10,1 e posteriores seguem os mesmos caminhos de atualização.

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado ou manual é…
9.15.1	9.16.1	direta
9.14.1	9.16.1	direta
	9.15.1	direta
9.13.1	9.16.1	direta
	9.15.1	direta
	9.14.1	direta
9.12.1	9.16.1	direta
	9.15.1	direta
	9.14.1	direta
	9.13.1	direta
9.11.1	9.16.1	multi-stage -9.11.1 → 9.15.1 -9.15.1 → 9.16.1
	9.15.1	direta
	9.14.1	direta
	9.13.1	direta
	9.12.1	direta

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado ou manual é…
9.10.1	9.16.1	multi-stage -9.10.1 → 9.14.1 -9.14.1 → 9.16.1
	9.15.1	multi-stage -9.10.1 → 9.14.1 -9.14.1 → 9.15.1
	9.14.1	direta
	9.13.1	direta
	9.12.1	direta
	9.11.1	direta

A partir de ONTAP 9.9,1

As atualizações automatizadas e manuais do ONTAP 9.9,1 seguem os mesmos caminhos de atualização.

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado ou manual é…
9.9.1	9.16.1	multi-stage -9,9.1→9.13.1 -9.13.1→9.16.1
	9.15.1	multi-stage -9,9.1→9.13.1 -9.13.1→9.15.1
	9.14.1	multi-stage -9,9.1→9.13.1 -9.13.1→9.14.1
	9.13.1	direta
	9.12.1	direta
	9.11.1	direta
	9.10.1	direta

A partir de ONTAP 9.8

As atualizações automatizadas e manuais do ONTAP 9.8 seguem os mesmos caminhos de atualização.

Se você estiver atualizando qualquer um dos seguintes modelos de plataforma em uma configuração IP do MetroCluster do ONTAP 9.8 para 9.10.1 ou posterior, primeiro você deve atualizar para o ONTAP 9.9,1:

- FAS2750
- FAS500f
- AFF A220
- AFF A250

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado ou manual é…
9,8	9.16.1	multi-stage -9,8 → 9.12.1 -9.12.1 → 9.16.1
9.15.1	multi-stage -9,8 → 9.12.1 -9.12.1 → 9.15.1	9.14.1

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado ou manual é…
multi-stage -9,8 → 9.12.1 -9.12.1 → 9.14.1	9.13.1	multi-stage -9,8 → 9.12.1 -9.12.1 → 9.13.1
9.12.1	direta	9.11.1
direta	9.10.1	direta

A partir de ONTAP 9.7

Os caminhos de atualização do ONTAP 9.7 podem variar dependendo se você está executando uma atualização automática ou manual.

Caminhos automatizados

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,7	9.16.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.16.1
	9.15.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.15.1
	9.14.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9,7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1
	9.11.1	multi-hop direto (requer imagens para 9,8 e 9.11.1)
	9.10.1	Multi-hop direto (requer imagens para 9,8 e 9.10.1P1 ou versão P posterior)
	9.9.1	direta
	9,8	direta

Caminhos manuais

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização manual é…
9,7	9.16.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.16.1
	9.15.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.15.1
	9.14.1	multi-stage -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9,7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,7 → 9,8 - 9,8 → 9.12.1
	9.11.1	multi-stage - 9,7 → 9,8 - 9,8 → 9.11.1
	9.10.1	multi-stage - 9,7 → 9,8 - 9,8 → 9.10.1
	9.9.1	direta
	9,8	direta

A partir de ONTAP 9.6

Os caminhos de atualização do ONTAP 9.6 podem variar dependendo se você está executando uma atualização automática ou manual.

Caminhos automatizados

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,6	9.16.1	multi-stage -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.16.1
	9.15.1	multi-stage -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.15.1
	9.14.1	multi-stage -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1	multi-stage - 9,6 → 9,8 -9,8 → 9.12.1
	9.11.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.11.1
	9.10.1	Multi-hop direto (requer imagens para 9,8 e 9.10.1P1 ou versão P posterior)
	9.9.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.9.1
	9,8	direta
	9,7	direta

Caminhos manuais

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização manual é…
9,6	9.16.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.16.1
	9.15.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.12.1
	9.11.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.11.1
	9.10.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.10.1
	9.9.1	multi-stage - 9,6 → 9,8 - 9,8 → 9.9.1
	9,8	direta
	9,7	direta

A partir de ONTAP 9.5

Os caminhos de atualização do ONTAP 9.5 podem variar dependendo se você está executando uma atualização automática ou manual.

Caminhos automatizados

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,5	9.16.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-hop direto (requer imagens para 9,7 e 9,9.1)
	9,8	multi-stage - 9,5 → 9,7 - 9,7 → 9,8
	9,7	direta
	9,6	direta

Caminhos de atualização manual

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização manual é…
9,5	9.16.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multi-stage - 9,5 → 9,7 - 9,7 → 9,8
	9,7	direta
	9,6	direta

De ONTAP 9.4-9,0

Os caminhos de atualização do ONTAP 9.4, 9,3, 9,2, 9,1 e 9,0 podem variar dependendo se você está executando uma atualização automática ou uma atualização manual.

Caminhos de atualização automatizados

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,4	9.16.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop direto, requer imagens para 9,7 e 9,9.1)
	9,8	multi-stage - 9,4 → 9,5 - 9,5 → 9,8 (multi-hop direto, requer imagens para 9,7 e 9,8)
	9,7	multi-stage - 9,4 → 9,5 - 9,5 → 9,7
	9,6	multi-stage - 9,4 → 9,5 - 9,5 → 9,6
	9,5	direta

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,3	9.16.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.10.1 (multi-hop direto, requer imagens para 9,8 e 9.10.1)
	9.9.1	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1
	9,8	multi-stage - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9,8
	9,7	multi-hop direto (requer imagens para 9,5 e 9,7)
	9,6	multi-stage - 9,3 → 9,5 - 9,5 → 9,6
	9,5	direta
	9,4	não disponível

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,2	9.16.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.10.1 (multi-hop direto, requer imagens para 9,8 e 9.10.1)
	9.9.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1
	9,8	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9,8
	9,7	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7)
	9,6	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multi-stage - 9,3 → 9,5 - 9,5 → 9,6
	9,4	não disponível
	9,3	direta

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,1	9.16.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9,8 - 9,8 → 9.12.1
	9.11.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.10.1 (multi-hop direto, requer imagens para 9,8 e 9.10.1)
	9.9.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1
	9,8	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9,8
	9,7	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7)
	9,6	multi-stage - 9,1 → 9,3 - 9,3 → 9,6 (multi-hop direto, requer imagens para 9,5 e 9,6)
	9,5	multi-stage - 9,1 → 9,3 - 9,3 → 9,5
	9,4	não disponível
	9,3	direta
	9,2	não disponível

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização automatizado é…
9,0	9.16.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.10.1 (multi-hop direto, requer imagens para 9,8 e 9.10.1)
	9.9.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9.9.1
	9,8	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7) - 9,7 → 9,8
	9,7	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop direto, requer imagens para 9,5 e 9,7)
	9,6	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5
	9,4	não disponível
	9,3	multi-stage - 9,0 → 9,1 - 9,1 → 9,3
	9,2	não disponível
	9,1	direta

Caminhos de atualização manual

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização ANDU é…
9,4	9.16.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.16.1
	9.15.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.15.1
	9.14.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multi-stage - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multi-stage - 9,4 → 9,5 - 9,5 → 9,7
	9,6	multi-stage - 9,4 → 9,5 - 9,5 → 9,6
	9,5	direta

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização ANDU é…
9,3	9.16.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.16.1
	9.15.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multi-stage - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multi-stage - 9,3 → 9,5 - 9,5 → 9,6
	9,5	direta
	9,4	não disponível

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização ANDU é…
9,2	9.16.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.16.1
	9.15.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multi-stage - 9,2 → 9,3 - 9,3 → 9,5
	9,4	não disponível
	9,3	direta

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização ANDU é…
9,1	9.16.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.16.1
	9.15.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multi-stage - 9,1 → 9,3 - 9,3 → 9,5
	9,4	não disponível
	9,3	direta
	9,2	não disponível

Se a sua versão atual do ONTAP for…	E seu lançamento de ONTAP alvo é…	Seu caminho de atualização ANDU é…
9,0	9.16.1	multi-estágios - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.16.1
	9.15.1	multi-estágios - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.15.1
	9.14.1	multi-estágios - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5
	9,4	não disponível
	9,3	multi-stage - 9,0 → 9,1 - 9,1 → 9,3
	9,2	não disponível
	9,1	direta

Data ONTAP 8

Certifique-se de que sua plataforma pode executar a versão de destino do ONTAP usando o "NetApp Hardware Universe".

Observação: o Guia de Atualização do Data ONTAP 8.3 afirma erroneamente que em um cluster de quatro nós, você deve Planejar atualizar o nó que contém o epsilon por último. Isso não é mais um requisito para atualizações a partir do Data ONTAP 8.2,3. Para obter mais informações, "NetApp Bugs Online Bug ID 805277"consulte .

A partir de Data ONTAP 8.3.x

Você pode atualizar diretamente para o ONTAP 9.1 e, em seguida, atualizar para versões posteriores.

A partir de versões do Data ONTAP anteriores a 8,3.x, incluindo 8,2.x

Você deve primeiro atualizar para o Data ONTAP 8.3.x, depois atualizar para o ONTAP 9.1 e, em seguida, atualizar para versões posteriores.

Verifique a configuração de failover de LIF

Antes de atualizar o ONTAP, você deve verificar se as políticas de failover e os grupos de failover do cluster estão configurados corretamente.

Durante o processo de atualização, os LIFs são migrados com base no método de atualização. Dependendo do método de atualização, a política de failover de LIF pode ou não ser usada.

Se você tiver 8 ou mais nós no cluster, a atualização automatizada será realizada usando o método batch. O método de atualização em lote envolve dividir o cluster em vários lotes de atualização, atualizar o conjunto de nós no primeiro lote, atualizar seus parceiros de alta disponibilidade (HA) e repetir o processo para os lotes restantes. No ONTAP 9.7 e anteriores, se o método de lote for usado, os LIFs serão migrados para o parceiro de HA do nó que está sendo atualizado. No ONTAP 9.8 e posterior, se o método batch for usado, LIFs são migrados para o outro grupo batch.

Se você tiver menos de 8 nós no cluster, a atualização automatizada será realizada usando o método contínuo. O método de atualização progressiva envolve iniciar uma operação de failover em cada nó em um par de HA, atualizar o nó que falhou, iniciar a giveback e repetir o processo para cada par de HA no cluster. Se o método contínuo for usado, os LIFs serão migrados para o nó de destino de failover conforme definido pela política de failover de LIF.

Passos

1. Exibir a política de failover para cada LIF de dados:

Se a sua versão do ONTAP for…	Use este comando
9,6 ou posterior	`network interface show -service-policy *data* -failover`
9,5 ou anterior	`network interface show -role data -failover`

   Este exemplo mostra a configuração de failover padrão para um cluster de dois nós com duas LIFs de dados:

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
                                           node1:e0f, node0:e0b,
                                           node0:e0c, node0:e0d,
                                           node0:e0e, node0:e0f
```

O campo **Failover Targets** mostra uma lista priorizada de destinos de failover para cada LIF. Por exemplo, se o 'lif0' falhar em sua porta inicial (e0b em node0), ele primeiro tentará fazer failover para a porta e0c em node0. Se o lif0 não puder falhar para e0c, ele então tentará fazer failover para a porta e0d no node0, e assim por diante.

2. Se a política de failover estiver definida como **Disabled** para quaisquer LIFs, exceto SAN LIFs, use o `network interface modify` comando para habilitar o failover.
3. Para cada LIF, verifique se o campo **Failover Targets** inclui portas de dados de um nó diferente que permanecerá ativo enquanto o nó inicial do LIF estiver sendo atualizado.

   Você pode usar o `network interface failover-groups modify` comando para adicionar um destino de failover ao grupo de failover.

   Exemplo

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

Informações relacionadas

"Gerenciamento de rede e LIF"

Verificar a configuração de roteamento SVM

Para evitar interrupções, antes de atualizar o software ONTAP, certifique-se de que a rota

SVM padrão seja capaz de alcançar qualquer endereço de rede que não seja acessível por uma rota mais específica. É uma prática recomendada configurar uma rota padrão para um SVM. Para obter mais informações, "SU134: O acesso à rede pode ser interrompido por uma configuração de roteamento incorreta no ONTAP"consulte .

A tabela de roteamento de um SVM determina o caminho de rede que o SVM usa para se comunicar com um destino. É importante entender como as tabelas de roteamento funcionam para que você possa evitar problemas de rede antes que eles ocorram.

As regras de roteamento são as seguintes:

- A ONTAP encaminha o tráfego para a rota mais específica disponível.
- O ONTAP roteia o tráfego por uma rota de gateway padrão (com 0 bits de máscara de rede) como último recurso, quando rotas mais específicas não estão disponíveis.

No caso de rotas com o mesmo destino, máscara de rede e métrica, não há garantia de que o sistema usará a mesma rota após uma reinicialização ou após uma atualização. Isso pode ser especialmente um problema se você tiver configurado várias rotas padrão.

Considerações especiais

Considerações especiais antes de uma atualização do ONTAP

Certas configurações de cluster exigem que você execute ações específicas antes de iniciar uma atualização de software do ONTAP. Por exemplo, se você tiver uma configuração de SAN, verifique se cada host está configurado com o número correto de caminhos diretos e indiretos antes de iniciar a atualização.

Consulte a tabela a seguir para determinar quais etapas adicionais você pode precisar tomar.

Antes de atualizar o ONTAP, pergunte a si mesmo…	**Se a sua resposta for sim, então faça isso…**
Meu cluster está atualmente em um estado de versão mista?	Verifique os requisitos de versão mista
Tenho uma configuração MetroCluster?	Revise os requisitos de atualização específicos para configurações do MetroCluster
Tenho uma configuração SAN?	Verifique a configuração do host SAN
Meu cluster tem relacionamentos SnapMirror definidos?	"Verifique a compatibilidade das versões do ONTAP para relacionamentos do SnapMirror"
Tenho relações SnapMirror do tipo DP definidas e estou atualizando para o ONTAP 9.12,1 ou posterior?	"Converta relacionamentos do tipo DP existentes para XDP"
Estou usando o SnapMirror S3 e estou atualizando para o ONTAP 9.12,1 ou posterior?	"Verifique o licenciamento para configurações do SnapMirror S3"
Utilizo uma relação SnapMirror e estou a atualizar do ONTAP 9.9,1 ou anterior para o 9.10.1 ou posterior?	"Desative snapshots de retenção de longo prazo em volumes intermediários de topologias em cascata"

Antes de atualizar o ONTAP, pergunte a si mesmo…	Se a sua resposta for sim, então faça isso…
Estou usando criptografia de armazenamento NetApp com servidores de gerenciamento de chaves externos?	Exclua todas as conexões existentes do servidor de gerenciamento de chaves
Tenho netgroups carregados em SVMs?	Verifique se o arquivo netgroup está presente em cada nó
Eu criei um SVM e estou atualizando do ONTAP 9.12,1 ou anterior para uma versão posterior?	Atribua um valor explícito à opção v4,2-xattrs
Tenho clientes LDAP usando o SSLv3?	Configurar clientes LDAP para usar TLS
Estou usando protocolos orientados para sessão?	Considerações de revisão para protocolos orientados para sessão
O modo SSL FIPS está habilitado em um cluster onde as contas de administrador se autenticam com uma chave pública SSH?	Verifique o suporte ao algoritmo da chave do host SSH
Minha proteção Autonomous ransomware tem um aviso ativo?	Responda aos avisos da Autonomous ransomware Protection sobre atividades anormais

Clusters ONTAP de versão mista

Um cluster de ONTAP de versão mista consiste em nós que executam duas versões principais diferentes do ONTAP por um tempo limitado. Por exemplo, se um cluster consiste atualmente em nós que executam o ONTAP 9.8 e 9.12.1, o cluster é um cluster de versão mista. Da mesma forma, um cluster no qual os nós estão executando o ONTAP 9.9,1 e o 9.13.1 seria um cluster de versão mista. O NetApp é compatível com clusters ONTAP de versão mista por períodos limitados de tempo e em cenários específicos.

A seguir estão os cenários mais comuns em que um cluster ONTAP estará em um estado de versão mista:

- Atualizações de software do ONTAP em clusters grandes
- São necessárias atualizações de software do ONTAP quando você planeja adicionar novos nós a um cluster

As informações se aplicam a versões do ONTAP que dão suporte a sistemas das plataformas NetApp, como os sistemas AFF A-Series e C-Series, ASA, FAS e C-series. As informações não se aplicam a versões de nuvem do ONTAP (9.x.0), como 9.12.0.

Requisitos para clusters ONTAP de versão mista

Se o cluster precisar inserir um estado de versão mista do ONTAP, você precisará estar ciente dos requisitos e restrições importantes.

- Não pode haver mais de duas versões principais diferentes do ONTAP em um cluster em um determinado momento. Por exemplo, ONTAP 9.9,1 e 9.13.1 são suportados, mas ONTAP 9.9,1, 9.12.1 e 9.13.1 não é. Os clusters com nós executados com diferentes níveis de patch P ou D da mesma versão do ONTAP, como ONTAP 9.9.1P1 e 9,9.1P5, não são considerados clusters de versão mista do ONTAP.

- Embora o cluster esteja em um estado de versão mista, você não deve inserir nenhum comando que altere a operação ou configuração do cluster, exceto aqueles que são necessários para o processo de atualização ou migração de dados. Por exemplo, atividades como (mas não limitadas a) migração de LIF, operações de failover de armazenamento planejadas ou criação ou exclusão de objetos em grande escala não devem ser realizadas até que a atualização e a migração de dados estejam concluídas.
- Para uma operação ideal do cluster, o período de tempo em que o cluster está em um estado de versão mista deve ser o mais curto possível. O período máximo de tempo que um cluster pode permanecer em um estado de versão mista depende da versão mais baixa do ONTAP no cluster.

Se a versão mais baixa do ONTAP em execução no cluster de versões mistas for:	Então você pode permanecer em um estado de versão mista por um máximo de
ONTAP 9 1.8 ou superior	90 dias
ONTAP 9 1.7 ou inferior	7 dias

- A partir do ONTAP 9.8, a diferença de versão entre os nós originais e os novos nós não pode ser maior que quatro. Por exemplo, um cluster ONTAP de versão mista pode ter nós executando o ONTAP 9.8 e 9.12.1, ou pode ter nós executando o ONTAP 9.9,1 e 9.13.1. No entanto, um cluster ONTAP de versão mista com nós executando o ONTAP 9.8 e 9.13.1 não seria suportado.

  Para obter uma lista completa de clusters de versões mistas compatíveis, "caminhos de atualização suportados"consulte . Todos os caminhos de atualização *Direct* são suportados para clusters de versões mistas.

Atualizando a versão do ONTAP de um cluster grande

Um cenário para inserir um estado de cluster de versão mista envolve a atualização da versão ONTAP de um cluster com vários nós para aproveitar os recursos disponíveis em versões posteriores do ONTAP 9. Quando você precisar atualizar a versão do ONTAP de um cluster maior, você entrará em um estado de cluster de versão mista por um período de tempo enquanto atualiza cada nó no cluster.

Adição de novos nós a um cluster do ONTAP

Outro cenário para inserir um estado de cluster de versão mista envolve a adição de novos nós ao cluster. Você pode adicionar novos nós ao cluster para expandir sua capacidade ou adicionar novos nós como parte do processo de substituição completa dos controladores. Em ambos os casos, você precisa habilitar a migração de seus dados de controladores existentes para os novos nós em seu novo sistema.

Se você pretende adicionar novos nós ao cluster e esses nós exigirem uma versão mínima do ONTAP posterior à versão atualmente em execução no cluster, será necessário realizar atualizações de software com suporte nos nós existentes no cluster antes de adicionar os novos nós.

Idealmente, você faria upgrade de todos os nós existentes para a versão mínima do ONTAP exigida pelos nós que pretende adicionar ao cluster. No entanto, se isso não for possível porque alguns dos seus nós existentes não suportam a versão posterior do ONTAP, você precisará inserir um estado de versão mista por um período limitado de tempo como parte do processo de atualização. Se você tiver nós que não suportem a versão mínima do ONTAP exigida pelos novos controladores, faça o seguinte:

1. "Atualização" Os nós que não oferecem suporte à versão mínima do ONTAP exigida pelos novos controladores para a versão máxima do ONTAP que eles oferecem suporte.

   Por exemplo, se você tiver um FAS8080 executando o ONTAP 9.5 e estiver adicionando uma nova plataforma C-Series executando o ONTAP 9.12,1, você deve atualizar seu FAS8080 para o ONTAP 9.8

(que é a versão máxima do ONTAP que ele suporta).

2. "Adicione os novos nós ao cluster".
3. "Migrar os dados" dos nós que estão sendo removidos do cluster para os nós recém-adicionados.
4. "Remova os nós não suportados do cluster".
5. "Atualização" os nós restantes no cluster para a mesma versão que os novos nós.

   Opcionalmente, atualize todo o cluster (incluindo seus novos nós) para a "lançamento de patch recomendado mais recente"versão do ONTAP em execução nos novos nós.

Para obter detalhes sobre migração de dados, consulte:

- "Crie um agregado e mova volumes para os novos nós"
- "Configuração de novas conexões iSCSI para movimentos de volume SAN"
- "Movimentação de volumes com criptografia"

Requisitos de atualização do ONTAP para configurações do MetroCluster

Antes de atualizar o software ONTAP em uma configuração do MetroCluster, os clusters precisam atender a certos requisitos.

- Ambos os clusters precisam estar executando a mesma versão do ONTAP.

  Você pode verificar a versão do ONTAP usando o comando version.

- Se você estiver executando uma atualização principal do ONTAP, a configuração do MetroCluster deve estar no modo normal.
- Se você estiver executando uma atualização do patch ONTAP, a configuração do MetroCluster pode estar no modo normal ou switchover.
- Para todas as configurações, exceto clusters de dois nós, é possível atualizar ambos os clusters sem interrupções ao mesmo tempo.

  Para a atualização sem interrupções em clusters de dois nós, os clusters precisam ser atualizados um nó de cada vez.

- Os agregados em ambos os clusters não podem estar no status RAID de ressincronização.

  Durante a recuperação de MetroCluster, os agregados espelhados são ressincronizados. Você pode verificar se a configuração do MetroCluster está nesse estado usando o `storage aggregate plex show -in-progress true` comando. Se algum agregado estiver sendo sincronizado, você não deve executar uma atualização até que a ressincronização esteja concluída.

- As operações de switchover negociadas falharão enquanto a atualização estiver em andamento.

  Para evitar problemas com operações de atualização ou reversão, não tente um switchover não planejado durante uma operação de atualização ou reversão, a menos que todos os nós em ambos os clusters estejam executando a mesma versão do ONTAP.

Requisitos de configuração para operação normal do MetroCluster

- Os LIFs do SVM de origem devem estar ativos e localizados em seus nós domésticos.

  Os LIFs de dados para as SVMs de destino não precisam estar ativos ou estar em seus nós iniciais.

- Todos os agregados no local devem estar online.
- Todos os volumes de raiz e de dados pertencentes às SVMs do cluster local devem estar online.

Requisitos de configuração para o switchover do MetroCluster

- Todos os LIFs devem estar ativos e localizados em seus nós domésticos.
- Todos os agregados precisam estar online, exceto os agregados de raiz no local de DR.

  Os agregados de raiz no local de DR ficam offline durante certas fases de switchover.

- Todos os volumes devem estar online.

Informações relacionadas

"Verificando o status de rede e armazenamento para configurações do MetroCluster"

Verifique a configuração do host SAN antes de uma atualização do ONTAP

A atualização do ONTAP em um ambiente SAN altera quais caminhos são diretos. Antes de atualizar um cluster SAN, verifique se cada host está configurado com o número correto de caminhos diretos e indiretos e se cada host está conetado aos LIFs corretos.

Passos

1. Em cada host, verifique se um número suficiente de caminhos diretos e indiretos está configurado e se cada caminho está ativo.

   Cada host deve ter um caminho para cada nó no cluster.

2. Verifique se cada host está conetado a um LIF em cada nó.

   Você deve gravar a lista de iniciadores para comparação após a atualização. Se você estiver executando o ONTAP 9.11,1 ou posterior, use o Gerenciador do sistema para exibir o status da conexão, pois ele oferece uma exibição muito mais clara do que a CLI.

System Manager

a. No System Manager, clique em **hosts > SAN Initiator Groups**.

   A página exibe uma lista de grupos de iniciadores (grupos de iniciadores). Se a lista for grande, você pode visualizar páginas adicionais da lista clicando nos números de página no canto inferior direito da página.

   As colunas exibem várias informações sobre os grupos. A partir de 9.11.1, o estado da ligação do grupo também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

CLI

◦ Listar iniciadores iSCSI:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

◦ Listar iniciadores FC:

```
fcp initiator show -fields igroup,wwpn,lif
```

SnapMirror

Versões compatíveis do ONTAP para relacionamentos do SnapMirror

Os volumes de origem e destino devem estar executando versões compatíveis do ONTAP antes de criar uma relação de proteção de dados do SnapMirror. Antes de atualizar o ONTAP, você deve verificar se sua versão atual do ONTAP é compatível com a versão de destino do ONTAP para relacionamentos do SnapMirror.

Relacionamentos de replicação unificada

Para relacionamentos SnapMirror do tipo "XDP", usando versões locais ou Cloud Volumes ONTAP:

Começando com ONTAP 9.9,0:

- As versões do ONTAP 9.x,0 são versões somente na nuvem e oferecem suporte a sistemas Cloud Volumes ONTAP. O asterisco (*) após a versão de lançamento indica uma versão somente na nuvem.

  O ONTAP 9.16,0 é uma exceção à regra somente de nuvem fornecendo suporte "Sistemas ASA R2"para o . Os sistemas ASA R2 suportam relações SnapMirror apenas com outros sistemas ASA R2.

- As versões do ONTAP 9.x,1 são versões gerais e oferecem suporte a sistemas locais e Cloud Volumes ONTAP.

Quando "balanceamento de capacidade avançado" o está ativado em volumes em clusters que executam o ONTAP 9.16.1 ou posterior, as transferências SnapMirror não são compatíveis com clusters que executam versões do ONTAP anteriores ao ONTAP 9.16.1.

A interoperabilidade é bidirecional.

Interoperabilidade para ONTAP versão 9,3 e posterior

Versão ONTAP…	**Interopera com essas versões anteriores do ONTAP…**																				
	9.16.1	9.16.0	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9,9.0*	9,8	9,7	9,6	9,5	9,4	9,3
9.16.1	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.16.0	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.15.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.15.0*	Não	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.14.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não
9.14.0*	Não	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.13.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não
9.13.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não
9.12.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não
9.12.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	Não	Não	Não	Não
9.11.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…																				
9.11.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.10.1	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.10.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.9.1	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,9.0*	Não	Não	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,8	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,7	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,6	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,5	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
9,4	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**
9,3	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**

Relações síncronas da SnapMirror

O SnapMirror síncrono não é compatível com instâncias de nuvem do ONTAP.

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…											
	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.16.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não
9.15.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não
9.14.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não

9.13.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.12.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.11.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não
9.10.1	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.9.1	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,8	Não	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não
9,7	Não	Não	Não	**Sim**	**Sim**	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
9,6	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**
9,5	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**

Relações de recuperação de desastres do SnapMirror SVM

Para dados de recuperação de desastres da SVM e proteção contra SVM:

A recuperação de desastres da SVM é compatível apenas entre clusters que executam a mesma versão do ONTAP. **A independência de versão não é suportada para replicação SVM**.

Na recuperação de desastres do SVM para migração SVM:

- A replicação é suportada em uma única direção de uma versão anterior do ONTAP na origem para a mesma ou posterior versão do ONTAP no destino.
- A versão do ONTAP no cluster de destino não deve ser mais do que duas versões principais no local mais recentes ou duas versões principais da nuvem mais recentes, como mostrado na tabela abaixo.
  - A replicação não é compatível com casos de uso de proteção de dados de longo prazo.

O asterisco (*) após a versão de lançamento indica uma versão somente na nuvem.

Para determinar o suporte, localize a versão de origem na coluna da tabela à esquerda e, em seguida, localize a versão de destino na linha superior (DR/migração para versões semelhantes e migração apenas para versões mais recentes).

Fonte	Destino																			
	9,3	9,4	9,5	9,6	9,7	9,8	9,9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1
9,3	DR/migração	Migração	Migração	Migração	Migração																	
9,4		DR/migração	Migração	Migração	Migração	Migração																

9,5			DR/migração	Migração	Migração	Migração	Migração														
9,6				DR/migração	Migração	Migração	Migração	Migração													
9,7					DR/migração	Migração	Migração	Migração	Migração												
9,8						DR/migração	Migração	Migração	Migração	Migração											
9,9.0*							DR/migração	Migração	Migração	Migração	Migração										
9.9.1								DR/migração	Migração	Migração	Migração	Migração									
9.10.0*									DR/migração	Migração	Migração	Migração	Migração								
9.10.1										DR/migração	Migração	Migração	Migração	Migração							
9.11.0*											DR/migração	Migração	Migração	Migração	Migração						
9.11.1												DR/migração	Migração	Migração	Migração	Migração					
9.12.0*													DR/migração	Migração	Migração	Migração	Migração				

9.12.1														DR/migração	Migração	Migração	Migração	Migração				
9.13.0*															DR/migração	Migração	Migração	Migração	Migração			
9.13.1																DR/migração	Migração	Migração	Migração	Migração		
9.14.0*																	DR/migração	Migração	Migração	Migração	Migração	
9.14.1																		DR/migração	Migração	Migração	Migração	Migração
9.15.0*																			DR/migração	Migração	Migração	Migração
9.15.1																				DR/migração	Migração	Migração
9.16.0																					DR/migração	Migração
9.16.1																						DR/migração

Relacionamentos de recuperação de desastres da SnapMirror

Para relações SnapMirror do tipo "DP" e do tipo de política "'assíncrono-mirror'":

Os espelhos do tipo DP não podem ser inicializados a partir do ONTAP 9.11,1 e são completamente obsoletos no ONTAP 9.12,1. Para obter mais informações, "Depreciação de relacionamentos SnapMirror de proteção de dados"consulte .

Na tabela a seguir, a coluna à esquerda indica a versão do ONTAP no volume de origem e a linha superior indica as versões do ONTAP que você pode ter no volume de destino.

Fonte	Destino											
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3	9,2	9,1	9
9.11.1	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.10.1	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.9.1	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não
9,8	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
9,7	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não
9,6	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
9,5	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não
9,4	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não
9,3	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não
9,2	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não
9,1	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não
9	Não	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim

A interoperabilidade não é bidirecional.

Converta uma relação de tipo DP existente para XDP no ONTAP

Se você estiver atualizando para o ONTAP 9.12,1 ou posterior, você deverá converter relações do tipo DP para XDP antes de atualizar. O ONTAP 9.12,1 e posterior não suporta relações do tipo DP. Você pode facilmente converter uma relação de tipo DP existente para XDP para aproveitar o SnapMirror flexível de versão.

Sobre esta tarefa

- O SnapMirror não converte automaticamente relacionamentos do tipo DP existentes para XDP. Para converter o relacionamento, você precisa quebrar e excluir o relacionamento existente, criar um novo relacionamento XDP e ressincronizar o relacionamento. Para obter informações de fundo, "O XDP substitui o DP como o padrão SnapMirror"consulte .
- Ao Planejar sua conversão, você deve estar ciente de que a preparação em segundo plano e a fase de armazenamento de dados de um relacionamento XDP SnapMirror podem levar muito tempo. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

Depois de converter um tipo de relacionamento SnapMirror de DP para XDP, as configurações relacionadas ao espaço, como dimensionamento automático e garantia de espaço, não são mais replicadas para o destino.

Passos

1. No cluster de destino, verifique se a relação SnapMirror é do tipo DP, se o estado do espelho é SnapMirrored, o status do relacionamento está ocioso e se o relacionamento está saudável:

```
snapmirror show -destination-path <SVM:volume>
```

O exemplo a seguir mostra a saída do `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

Você pode achar útil manter uma cópia da[`snapmirror show` saída do comando para manter o controle existente das configurações de relacionamento. Saiba mais sobre o comando `snapmirror show` na referência de comando ONTAP.

2. A partir dos volumes de origem e destino, verifique se ambos os volumes têm uma cópia Snapshot comum:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra a `volume snapshot show` saída para os volumes de origem e destino:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantir que as atualizações agendadas não sejam executadas durante a conversão, execute o relacionamento existente do tipo DP:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-quiesce.html[`snapmirror quiesce`(em inglês) na referência de comando ONTAP.

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir anula a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` em `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Quebre a relação existente do tipo DP:

```
snapmirror break -destination-path <SVM:volume>
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-break.html[`snapmirror-break`(em inglês) na referência de comando ONTAP .

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir rompe a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Se a exclusão automática de cópias Snapshot estiver ativada no volume de destino, desative-a:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

O exemplo a seguir desativa a cópia snapshot autodelete no volume de `volA_dst` destino :

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Eliminar a relação do tipo DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-delete.html[`snapmirror-delete`(em inglês) na referência de comando ONTAP.

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir exclui a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Solte a relação de recuperação de desastres do SVM de origem na fonte:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

O exemplo a seguir libera a relação de recuperação de desastres da SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. Você pode usar a saída que reteve do `snapmirror show` comando para criar a nova relação do tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

O novo relacionamento deve usar o mesmo volume de origem e destino. Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir cria uma relação de recuperação de desastres do SnapMirror entre o volume de origem `volA` ligado `svm1` e o volume de `volA_dst` destino ligado `svm_backup` usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Ressincronizar os volumes de origem e destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para melhorar o tempo de ressincronização, você pode usar a `-quick-resync` opção, mas deve estar ciente de que a economia com eficiência de storage pode ser perdida. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-resync.html n.o parameters.html[`snapmirror resync` na referência de comando ONTAP.

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Se a exclusão automática de cópias Snapshot for desativada, reative-a:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Depois de terminar

1. Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada.
2. Quando o volume de destino XDP do SnapMirror começar a atualizar cópias Snapshot conforme definido pela política SnapMirror, use a saída `snapmirror list-destinations` do comando do cluster de origem para exibir a nova relação XDP do SnapMirror.

Desative snapshots de retenção de longo prazo antes da atualização do ONTAP

Se você estiver atualizando do ONTAP 9.9,1 ou anterior para o ONTAP 9.10,1 ou posterior e tiver uma relação em cascata do SnapMirror configurada no cluster, desative os snapshots de retenção de longo prazo (LTR) de volumes intermediários na cascata antes de atualizar. Em cascata um volume com instantâneos LTR ativados não é suportado no ONTAP 9.10,1 ou posterior. O uso dessa configuração após a atualização pode resultar em backups e snapshots perdidos.

Você precisa agir nos seguintes cenários:

- Os instantâneos de retenção de longo prazo (LTR) são configurados no volume "B" em uma cascata SnapMirror **A › B › C** ou em outro volume de destino SnapMirror médio em sua cascata maior.
- Os instantâneos LTR são definidos por uma programação aplicada a uma regra de política do SnapMirror. Essa regra não replica snapshots do volume de origem, mas os cria diretamente no volume de destino.

Para obter mais informações sobre horários e políticas do SnapMirror, consulte o artigo da base de dados de Conhecimento "Como funciona o parâmetro "schedule" em uma regra de política do ONTAP 9 SnapMirror?" .

Passos

1. Remova a regra LTR da política SnapMirror no volume médio da cascata:

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
-snapmirror-label <>
```

2. Adicione a regra novamente para a etiqueta SnapMirror sem a programação LTR:

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>
-snapmirror-label <> -keep <>
```

A remoção de instantâneos LTR das regras de política do SnapMirror significa que o SnapMirror irá retirar os instantâneos com o rótulo fornecido do volume de origem. Também pode ser necessário adicionar ou modificar uma programação na política de instantâneos do volume de origem para criar instantâneos devidamente rotulados.

3. Se necessário, modifique (ou crie) um agendamento na política de instantâneos do volume de origem para permitir que os instantâneos sejam criados com um rótulo SnapMirror:

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

Os instantâneos LTR ainda podem ser ativados no volume de destino final do SnapMirror dentro de uma configuração em cascata do SnapMirror.

Verifique o licenciamento para configurações do SnapMirror S3

Antes de atualizar o ONTAP, se estiver a utilizar o SnapMirror S3 e estiver a atualizar para o ONTAP 9.12,1 ou posterior, deve verificar se tem as licenças SnapMirror adequadas.

Após a atualização do ONTAP, as alterações de licenciamento que ocorreram entre o ONTAP 9.11,1 e anterior e o ONTAP 9.12,1 e posterior podem causar falha nas relações do SnapMirror S3.

ONTAP 9.11,1 e anteriores

- Ao replicar para um bucket de destino hospedado no NetApp (ONTAP S3 ou StorageGRID), o SnapMirror S3 verifica a licença síncrona do SnapMirror, incluída no pacote de proteção de dados antes da introdução do "ONTAP One"pacote de software.
- Ao replicar para um bucket de destino que não seja da NetApp, o SnapMirror S3 verifica a licença de nuvem do SnapMirror, incluída no pacote de nuvem híbrida, que estava disponível antes da introdução do "ONTAP One"pacote de software.

ONTAP 9.12,1 e posterior

- Ao replicar para um bucket de destino hospedado no NetApp (ONTAP S3 ou StorageGRID), o SnapMirror S3 verifica a licença do SnapMirror S3, incluída no pacote de proteção de dados que estava disponível antes da introdução do "ONTAP One" pacote de software.
- Ao replicar para um bucket de destino que não seja da NetApp, o SnapMirror S3 verifica se há licença externa do SnapMirror S3, incluída no pacote de nuvem híbrida que estava disponível antes da introdução do "ONTAP One"pacote de software e do "Pacote de compatibilidade ONTAP One".

Relações existentes do SnapMirror S3

As relações existentes do SnapMirror S3 devem continuar a funcionar após uma atualização do ONTAP 9.11,1 ou anterior para o ONTAP 9.12,1 ou posterior, mesmo que o cluster não tenha o novo licenciamento.

A criação de novas relações do SnapMirror S3 falhará se o cluster não tiver a licença adequada instalada.

Exclua conexões existentes do servidor de gerenciamento de chaves externas antes de atualizar o ONTAP

Antes de atualizar o ONTAP, se você estiver executando o ONTAP 9.2 ou anterior com o NetApp Storage Encryption (NSE) e atualizando para o ONTAP 9.3 ou posterior, use a interface de linha de comando (CLI) para excluir quaisquer conexões de servidor de gerenciamento de chaves externas (KMIP) existentes.

Passos

1. Verifique se as unidades do NSE estão desbloqueadas, abertas e definidas para a ID segura de fabricação padrão 0x0:

```
storage encryption disk show -disk *
```

2. Entre no modo de privilégio avançado:

```
set -privilege advanced
```

3. Use a ID segura de fabricação padrão 0x0 para atribuir a chave FIPS aos discos de criptografia automática (SEDs):

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. Verifique se a atribuição da chave FIPS a todos os discos está concluída:

```
storage encryption disk show-status
```

5. Verifique se o **mode** para todos os discos está definido como dados

```
storage encryption disk show
```

6. Exibir os servidores KMIP configurados:

```
security key-manager show
```

7. Exclua os servidores KMIP configurados:

```
security key-manager delete -address <kmip_ip_address>
```

8. Exclua a configuração do gerenciador de chaves externo:

```
security key-manager delete-kmip-config
```

Esta etapa não remove os certificados NSE.

O que vem a seguir

Depois que a atualização estiver concluída, você deve Reconfigure as conexões do servidor KMIP.

Verifique se o arquivo netgroup está presente em todos os nós antes de uma atualização do ONTAP

Antes de atualizar o ONTAP, se você tiver carregado netgroups em máquinas virtuais de armazenamento (SVMs), verifique se o arquivo netgroup está presente em cada nó. Um arquivo netgroup ausente em um nó pode causar falha na atualização.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Exibir o status do netgroup para cada SVM:

```
vserver services netgroup status
```

3. Verifique se, para cada SVM, cada nó mostra o mesmo valor de hash de arquivo netgroup:

```
vserver services name-service netgroup status
```

Se for esse o caso, você pode pular a próxima etapa e prosseguir com a atualização ou reversão. Caso contrário, avance para o passo seguinte.

4. Em qualquer nó do cluster, carregue manualmente o arquivo netgroup:

```
vserver services netgroup load -vserver vserver_name -source uri
```

Este comando faz o download do arquivo netgroup em todos os nós. Se um arquivo netgroup já existir em um nó, ele será substituído.

Informações relacionadas

"Trabalhando com Netgroups"

Atribua um valor explícito à opção v4,2-xattrs

Se você tiver um cliente NFSv4,2, antes de atualizar a partir de certas versões e patches do ONTAP 9.12,1 e posteriores, você precisa dar um valor explícito para a opção NFSv4,2 Extended Attributes para evitar erros de resposta NFS após a atualização.

Se a `v4.2-xattrs` opção nunca for explicitamente atribuído um valor antes da atualização do ONTAP para versões afetadas, os clientes NFSv4,2 não serão informados de que a opção de atributos estendidos do servidor foi alterada. Isso causa erros de resposta NFS a chamadas específicas `xattrs` devido a uma incompatibilidade de cliente e servidor.

Antes de começar

Você precisa atribuir um valor explícito para a opção NFSv4,2 atributos estendidos se o seguinte for verdadeiro:

- Você está usando o NFSv4,2 com um SVM criado usando o ONTAP 9.11,1 ou anterior
- Você está atualizando o ONTAP de qualquer uma dessas versões e patches afetados:
  - 9.12.1RC1 a 9.12.1P11
  - 9.13.1RC1 a 9.13.1P8
  - 9.14.1RC1 a 9.14.1P1

Sobre esta tarefa

Você deve estar executando o ONTAP 9.12,1 ou posterior para definir o valor usando o comando descrito neste procedimento.

Se `v4.2-xattrs` já estiver definido como `enabled`, ele ainda deve ser explicitamente definido como `enabled` para evitar interrupções futuras. Se você definir `v4.2-xattrs` como desativado, os clientes NFSv4,2 podem receber respostas "argumento inválido" até que sejam remontados ou a `v4.2-xattrs` opção esteja definida como `enabled`.

Passos

- Atribua um valor explícito à `v4.2-xattrs` opção:

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

Informações relacionadas

"O campo NFS v4,2-xattrs está sendo virado após atualizações"

Configure os clientes LDAP para usar TLS para maior segurança

Antes de atualizar o ONTAP, você deve configurar clientes LDAP usando o SSLv3 para comunicações seguras com servidores LDAP para usar o TLS. O SSL não estará disponível após a atualização.

Por padrão, as comunicações LDAP entre aplicativos cliente e servidor não são criptografadas. Você deve proibir o uso de SSL e impor o uso de TLS.

Passos

1. Verifique se os servidores LDAP no seu ambiente suportam TLS.

   Se não o fizerem, não prossiga. Você deve atualizar seus servidores LDAP para uma versão que suporte TLS.

2. Verifique quais configurações de cliente LDAP do ONTAP têm LDAP em SSL/TLS ativado:

   ```
   vserver services name-service ldap client show
   ```

   Se não houver nenhum, você pode pular os passos restantes. No entanto, você deve considerar o uso de LDAP sobre TLS para melhor segurança.

3. Para cada configuração de cliente LDAP, desative o SSL para impor o uso de TLS:

   ```
   vserver services name-service ldap client modify -vserver <vserver_name>
   -client-config <ldap_client_config_name> -allow-ssl false
   ```

4. Verifique se o uso de SSL não é mais permitido para nenhum cliente LDAP:

   ```
   vserver services name-service ldap client show
   ```

Informações relacionadas

"Gerenciamento de NFS"

Considerações para protocolos orientados para sessão

Clusters e protocolos orientados para sessões podem causar efeitos adversos a clientes e aplicações em determinadas áreas, como serviço de e/S durante as atualizações.

Se você estiver usando protocolos orientados para sessão, considere o seguinte:

- SMB

  Se você fornecer compartilhamentos de CA (continuamente disponíveis) com o SMBv3, poderá usar o método de atualização sem interrupções automatizado (com o System Manager ou a CLI) e não haverá interrupção pelo cliente.

  Se você estiver fornecendo compartilhamentos com SMBv1 ou SMBv2 ou compartilhamentos não CA com SMBv3, as sessões do cliente serão interrompidas durante as operações de aquisição e reinicialização de atualização. Você deve direcionar os usuários para terminar suas sessões antes de atualizar.

  O Hyper-V e o SQL Server sobre SMB são compatíveis com operações ininterruptas (NDOs). Se você configurou uma solução Hyper-V ou SQL Server em SMB, os servidores de aplicativos e as máquinas virtuais ou bancos de dados contidos permanecem on-line e fornecem disponibilidade contínua durante a atualização do ONTAP.

- NFSv4.x

  Os clientes NFSv4.x recuperarão automaticamente de perdas de conexão experimentadas durante a atualização usando procedimentos normais de recuperação NFSv4.x. Os aplicativos podem sofrer um atraso temporário de e/S durante esse processo.

- NDMP

  O estado é perdido e o usuário do cliente deve tentar novamente a operação.

- Backups e restaurações

  O estado é perdido e o usuário do cliente deve tentar novamente a operação.

  > Não inicie um backup ou restauração durante ou imediatamente antes de uma atualização. Isso pode resultar em perda de dados.

- Aplicativos (por exemplo, Oracle ou Exchange)

  Os efeitos dependem das aplicações. Para aplicativos baseados em tempo limite, você pode ser capaz de alterar a configuração de tempo limite para mais tempo do que o tempo de reinicialização do ONTAP para minimizar os efeitos adversos.

Verifique o suporte do algoritmo da chave do host SSH antes da atualização do ONTAP

Antes de atualizar o ONTAP, se o modo SSL FIPS estiver ativado em um cluster onde as contas de administrador se autenticam com uma chave pública SSH, você deve garantir que o algoritmo de chave do host seja suportado na versão de ONTAP de destino.

A tabela a seguir indica algoritmos de tipo de chave de host compatíveis com conexões SSH ONTAP. Esses tipos de chave não se aplicam à configuração da autenticação pública SSH.

Lançamento do ONTAP	Tipos de chave compatíveis no modo FIPS	Tipos de chave compatíveis no modo não FIPS
9.11.1 e mais tarde	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 e rsa-sha2-512 e rsa-sha2-256 e ssh-ed25519 e ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss e ssh-rsa

O suporte para o algoritmo de chave de host ssh-ed25519 é removido a partir de ONTAP 9.11,1.

Para obter mais informações, "Configurar a segurança da rede usando o FIPS"consulte .

Contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado antes de atualizar ou a autenticação de administrador falhar.

"Saiba mais sobre como ativar contas de chave pública SSH."

Responder a avisos anormais de atividade no Autonomous ransomware Protection (ARP)

Antes de atualizar para o ONTAP 9.16,1 ou posterior, você deve responder a quaisquer avisos de atividade anormais relatados pela proteção Autônoma contra ransomware (ARP). No ONTAP 9.16,1, o ARP mudou para um modelo baseado em aprendizado de máquina/inteligência artificial (IA). Devido a essa alteração, quaisquer avisos ativos não resolvidos do ARP existente no ONTAP 9.15,1 ou anterior serão perdidos após a atualização.

Passos

1. Responda a quaisquer avisos de atividade anormais comunicados pela "ARP" e resolva quaisquer problemas potenciais.
2. Confirme a resolução desses problemas antes de atualizar selecionando **Atualizar e Limpar tipos de arquivos suspeitos** para Registrar sua decisão e retomar o monitoramento ARP normal.

Reinicie o SP ou o BMC para se preparar para a atualização de firmware durante uma atualização do ONTAP

Não é necessário atualizar manualmente o firmware antes de efetuar uma atualização do ONTAP. O firmware do cluster está incluído no pacote de atualização do ONTAP e é copiado para o dispositivo de inicialização de cada nó. O novo firmware é então instalado como parte do processo de atualização.

O firmware dos seguintes componentes é atualizado automaticamente se a versão do cluster for mais antiga do que o firmware fornecido com o pacote de atualização do ONTAP:

- BIOS/Loader
- Processador de Serviço (SP) ou controlador de gerenciamento de placa base (BMC)
- Compartimento de armazenamento

- Disco
- Flash Cache

Para se preparar para uma atualização suave, você deve reiniciar o SP ou o BMC antes que a atualização comece.

Passo

1. Reinicie o SP ou o BMC antes da atualização:

```
system service-processor reboot-sp -node <node_name>
```

   Reinicie apenas um SP ou BMC de cada vez. Aguarde que o SP ou BMC reinicializado recicle completamente antes de reiniciar o próximo.

Você também pode "atualize o firmware manualmente"fazer o mesmo entre as atualizações do ONTAP. Se tiver o Digital Advisor, pode "Veja a lista de versões de firmware atualmente incluídas na imagem do ONTAP".

Versões de firmware atualizadas estão disponíveis da seguinte forma:

- "Firmware do sistema (BIOS, BMC, SP)"
- "Firmware do compartimento"
- "Firmware de cache de disco e Flash"

Transfira a imagem do software ONTAP

Antes de atualizar o ONTAP, primeiro você deve baixar a imagem de software ONTAP de destino no site de suporte da NetApp. Dependendo da versão do ONTAP, você pode baixar o software ONTAP para um servidor HTTPS, HTTP ou FTP em sua rede ou para uma pasta local.

Se você está correndo…	Você pode baixar a imagem para este local…
ONTAP 9 F.6 e mais tarde	• Um servidor HTTPS com o certificado CA do servidor deve ser instalado no sistema local. • Uma pasta local • Um servidor HTTP ou FTP
ONTAP 9 .4 e mais tarde	• Uma pasta local • Um servidor HTTP ou FTP
ONTAP 9 F.0 e mais tarde	Um servidor HTTP ou FTP

Sobre esta tarefa

- Se você estiver executando uma atualização sem interrupções automatizada (ANDU) usando um "caminho de atualização direta de multi-hop", precisará "transferir"do pacote de software para a versão intermediária do ONTAP e para a versão ONTAP de destino necessária para sua atualização. Por exemplo, se você estiver atualizando do ONTAP 9.8 para o ONTAP 9.13,1, você deve baixar os pacotes

de software para ONTAP 9.12,1 e ONTAP 9.13,1. "caminhos de atualização suportados"Consulte para determinar se o caminho de atualização requer que você baixe um pacote de software intermediário.

- Se estiver a atualizar um sistema com encriptação de volume NetApp para o ONTAP 9.5 ou posterior, tem de transferir a imagem do software ONTAP para países não restritos, que inclui encriptação de volume NetApp.

  Se você usar a imagem do software ONTAP para países restritos para atualizar um sistema com criptografia de volume NetApp, o sistema ficará em pânico e perderá o acesso aos volumes.

- Não é necessário transferir um pacote de software separado para o seu firmware. A atualização de firmware do cluster está incluída no pacote de atualização do software ONTAP e é copiada para o dispositivo de inicialização de cada nó. O novo firmware é então instalado como parte do processo de atualização.

Passos

1. Localize o software ONTAP de destino na "Transferências de software" área do site de suporte da NetApp.

   Para uma atualização do ONTAP Select, selecione **Atualização do nó ONTAP Select**.

2. Copie a imagem do software (por exemplo, 97_q_image.tgz) para o local apropriado.

   Dependendo da versão do ONTAP, o local será um diretório de um servidor HTTP, HTTPS ou FTP a partir do qual a imagem será servida ao sistema local ou a uma pasta local no sistema de armazenamento.

Métodos de atualização do ONTAP

Métodos de atualização do software ONTAP

Você pode fazer uma atualização automatizada do software ONTAP usando o Gerenciamento do sistema. Como alternativa, você pode executar uma atualização automática ou manual usando a interface de linha de comando (CLI) do ONTAP. O método usado para atualizar o ONTAP depende da configuração, da versão atual do ONTAP e do número de nós no cluster. A NetApp recomenda o uso do Gerenciador de sistemas para realizar atualizações automatizadas, a menos que sua configuração exija uma abordagem diferente. Por exemplo, se você tiver uma configuração do MetroCluster com 4 nós executando o ONTAP 9.3 ou posterior, use o Gerenciador de sistema para realizar uma atualização automatizada (às vezes chamada de atualização sem interrupções automatizada ou ANDU). Se você tiver uma configuração do MetroCluster com 8 nós executando o ONTAP 9.2 ou anterior, use a CLI para realizar uma atualização manual.

Se estiver a atualizar para o ONTAP 9.15,1 ou posterior através do BlueXP , siga o "Procedimento de atualização na documentação do BlueXP ".

Uma atualização pode ser executada usando o processo de atualização contínua ou o processo de atualização em lote. Ambos não causam interrupções.

Para atualizações automatizadas, o ONTAP instala automaticamente a imagem ONTAP de destino em cada nó, valida os componentes do cluster para garantir que o cluster possa ser atualizado sem interrupções e, em seguida, executa uma atualização em lote ou contínua em segundo plano com base no número de nós. Para

atualizações manuais, o administrador confirma manualmente que cada nó no cluster está pronto para atualização e, em seguida, executa as etapas para executar uma atualização contínua.

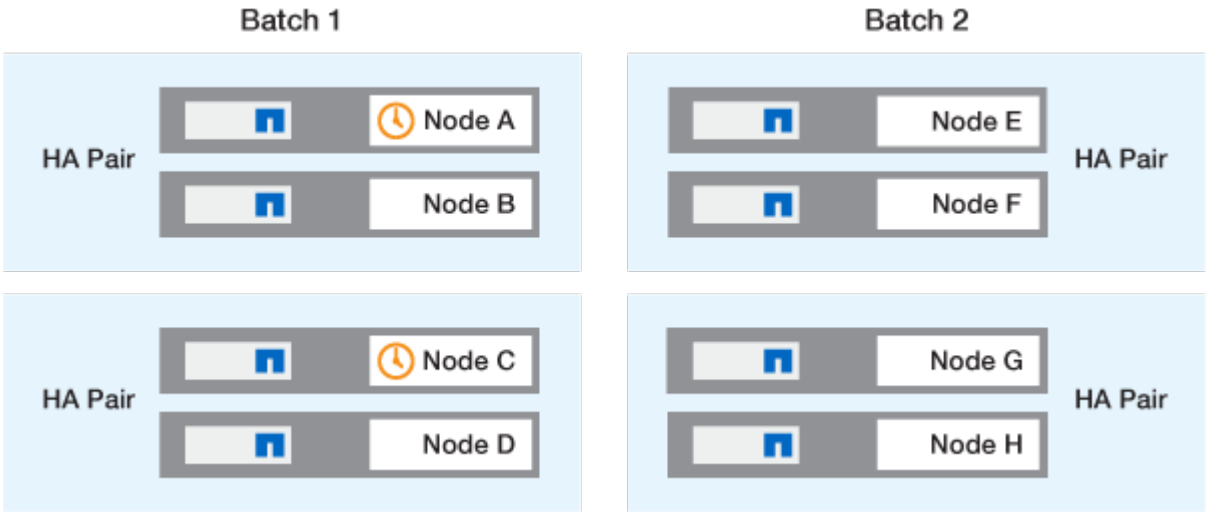
Atualizações contínuas do ONTAP

O processo de atualização progressiva é o padrão para clusters com menos de 8 nós. No processo de atualização contínua, um nó é colocado offline e atualizado enquanto seu parceiro assume seu armazenamento. Quando a atualização do nó estiver concluída, o nó do parceiro devolverá o controle ao nó proprietário original, e o processo será repetido no nó do parceiro. Cada par de HA adicional é atualizado em sequência até que todos os pares de HA estejam executando a versão de destino.

Atualizações em lote do ONTAP

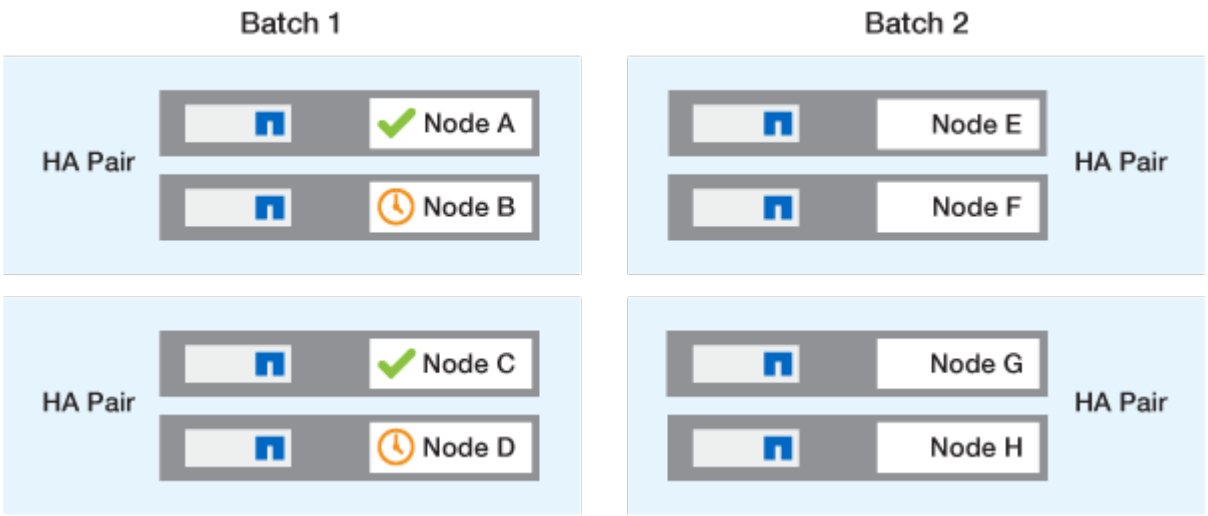
O processo de atualização em lote é o padrão para clusters de 8 nós ou mais. No processo de atualização em lote, o cluster é dividido em dois lotes. Cada lote contém vários pares de HA. No primeiro lote, o primeiro nó de cada par de HA é atualizado simultaneamente com o primeiro nó de todos os outros pares de HA no lote.

No exemplo a seguir, há dois pares de HA em cada lote. Quando a atualização em lote começa, o nó A e o nó C são atualizados simultaneamente.



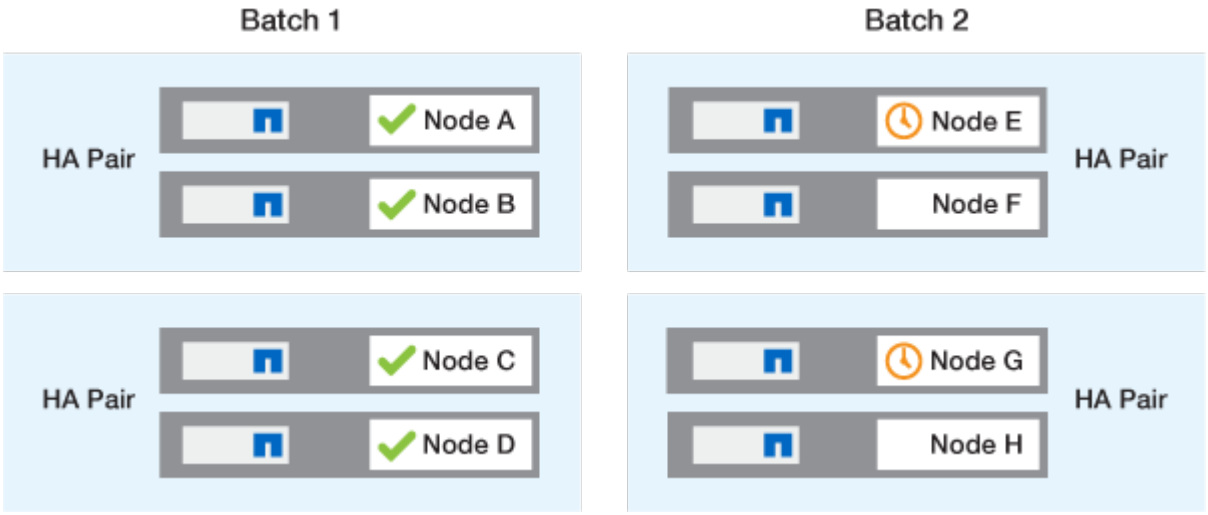
Após a atualização dos primeiros nós de cada par de HA ser concluída, os nós de parceiros no lote 1 são atualizados simultaneamente.

No exemplo a seguir, depois que o nó A e o nó C são atualizados, o nó B e o nó D são atualizados simultaneamente.



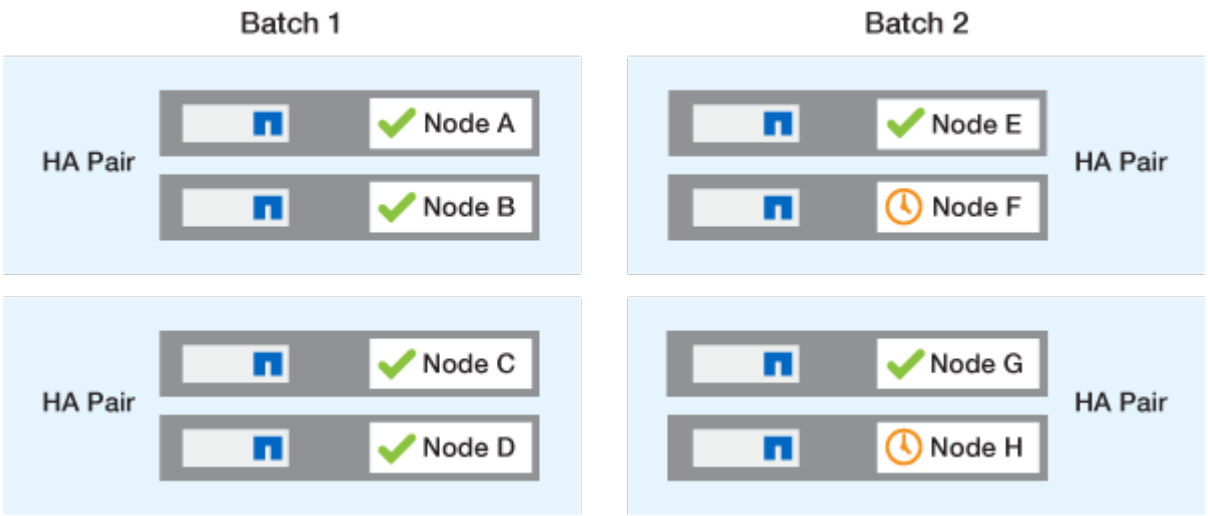
O processo é repetido para os nós no lote 2. O primeiro nó de cada par de HA é atualizado simultaneamente com o primeiro nó de todos os outros pares de HA no lote.

No exemplo a seguir, o nó e e o nó G são atualizados simultaneamente.



Após a atualização dos primeiros nós de cada par de HA ser concluída, os nós de parceiros no lote 2 são atualizados simultaneamente.

No exemplo a seguir, o nó F e o nó H são atualizados simultaneamente para concluir o processo de atualização em lote.



Métodos de atualização recomendados do ONTAP com base na configuração

Os métodos de atualização suportados pela sua configuração estão listados por ordem de utilização recomendada.

Configuração	Versão de ONTAP	Número de nós	Método de atualização recomendado
Padrão	9,0 ou posterior	2 ou mais	• Sem interrupções automatizadas com o System Manager • Sem interrupções automatizadas com a CLI
Padrão	9,0 ou posterior	Único	"Interrupções automatizadas"
MetroCluster	9,3 ou posterior	8	• Sem interrupções automatizadas com a CLI • Sem interrupções manuais para MetroCluster de 4 ou 8 nós usando a CLI
MetroCluster	9,3 ou posterior	2,4	• Sem interrupções automatizadas com o System Manager • Sem interrupções automatizadas com a CLI
MetroCluster	9,2 ou anterior	4, 8	Sem interrupções manuais para MetroCluster de 4 ou 8 nós usando a CLI
MetroCluster	9,2 ou anterior	2	Sem interrupções manuais para MetroCluster de 2 nós usando a CLI

ANDU usando o System Manager é o método de atualização recomendado para todas as atualizações de patch, independentemente da configuração.

Um atualização disruptiva manual pode ser executado em qualquer configuração. No entanto, você não deve executar uma atualização disruptiva a menos que você possa colocar o cluster offline durante a atualização. Se estiver operando em um ambiente SAN, você deverá estar preparado para encerrar ou suspender todos os clientes SAN antes de executar uma atualização disruptiva. As atualizações disruptivas são realizadas usando a CLI do ONTAP.

Atualização automatizada sem interrupções de ONTAP

Quando você executa uma atualização automatizada, o ONTAP instala automaticamente a imagem ONTAP de destino em cada nó, valida que o cluster pode ser atualizado com

sucesso e, em seguida, executa um atualização em lote ou contínuaem segundo plano com base no número de nós no cluster.

Se for suportado pela sua configuração, você deve usar o System Manager para executar uma atualização automatizada. Se sua configuração não oferecer suporte a atualização automatizada usando o Gerenciador de sistema, você poderá usar a interface de linha de comando (CLI) do ONTAP para realizar uma atualização automatizada.

Se estiver a atualizar para o ONTAP 9.15,1 ou posterior através do BlueXP , siga o "Procedimento de atualização na documentação do BlueXP ".

Modificar a configuração da `storage failover modify-auto-giveback` opção de comando antes do início de uma atualização automática sem interrupções (ANDU) não tem impactos no processo de atualização. O processo ANDU ignora qualquer valor predefinido para esta opção durante a aquisição/giveback necessário para a atualização. Por exemplo, definir `-autogiveback` como false antes do início ANDU não interrompe a atualização automática antes da giveback.

Antes de começar

- Você deve "prepare-se para o seu upgrade".
- Você deve "Transfira a imagem do software ONTAP" para o seu lançamento de ONTAP de destino.

  Se estiver a executar um "atualização direta de multi-hop", tem de transferir ambas as imagens ONTAP necessárias para o seu específico "caminho de atualização".

- Para cada par de HA, cada nó deve ter uma ou mais portas no mesmo domínio de broadcast.

  Se o cluster do ONTAP tiver 8 ou mais nós, o método de atualização em lote será usado na atualização sem interrupções automática para forçar preventivamente a migração de LIF de dados antes da takeover do SFO. A forma como os LIFs são migrados durante uma atualização em lote varia de acordo com a sua versão do ONTAP.

Se você estiver executando o ONTAP…	LIFs são migrados…
• 9.15.1 ou posterior • 9.14.1P5 • 9.13.1P10 • 9.12.1P13 • 9.11.1P16, P17 • 9.10.1P19	Para um nó no outro grupo de lote. Se a migração para o outro grupo de lote falhar, os LIFs serão migrados para o parceiro de HA do nó no mesmo grupo de lote.
9,8 a 9.14.1	Para um nó no outro grupo de lote. Se o domínio de transmissão de rede não permitir a migração de LIF para o outro grupo de lote, a migração de LIF falha e ANDU pausa.
9,7 ou anterior	Para o parceiro de HA do nó que está sendo atualizado. Se o parceiro não tiver portas no mesmo domínio de broadcast, a migração de LIF falhará e ANDU parará.

- Se você estiver atualizando o ONTAP em uma configuração MetroCluster FC, o cluster deve estar habilitado para switchover automático não planejado.
- Se não pretende monitorizar o progresso do processo de atualização, deve "Solicite notificações EMS de erros que possam exigir intervenção manual".
- Se você tiver um cluster de nó único, siga o "atualização sem interrupções automatizada" processo.

  As atualizações de clusters de nó único causam interrupções.

Exemplo 2. Passos

System Manager

1. Valide a imagem de destino ONTAP:

   Se você estiver atualizando uma configuração do MetroCluster, valide o cluster A e repita o processo de validação no cluster B.

   a. Dependendo da versão do ONTAP que você está executando, execute uma das seguintes etapas:

Se você está correndo…	Faça isso…
ONTAP 9 .8 ou posterior	Clique em **Cluster > Overview**.
ONTAP 9.5, 9,6 e 9,7	Clique em **Configuração** > **Cluster** > **Atualizar**.
ONTAP 9 .4 ou anterior	Clique em **Configuração** > **Atualização de cluster**.

   b. No canto direito do painel **Visão geral**, clique em .

   c. Clique em **Atualização do ONTAP**.

   d. Na guia **Atualização de cluster**, adicione uma nova imagem ou selecione uma imagem disponível.

Se você quiser…	Então…
Adicione uma nova imagem de software a partir de uma pasta local Você já deve ter "transferir a imagem"para o cliente local.	i. Em **imagens de software disponíveis**, clique em **Adicionar do local**. ii. Navegue até o local onde você salvou a imagem do software, selecione a imagem e clique em **Open**.
Adicione uma nova imagem de software a partir de um servidor HTTP ou FTP	i. Clique em **Adicionar do servidor**. ii. Na caixa de diálogo **Adicionar uma nova imagem de software**, insira o URL do servidor HTTP ou FTP para o qual você baixou a imagem do software ONTAP do site de suporte da NetApp. Para FTP anônimo, você deve especificar a URL no ftp://anonymous@ftpserver formato. iii. Clique em **Add**.
Selecione uma imagem disponível	Escolha uma das imagens listadas.

e. Clique em **Validar** para executar as verificações de validação de pré-atualização.

   Se forem encontrados erros ou avisos durante a validação, estes são apresentados juntamente com uma lista de acões correctivas. Você deve resolver todos os erros antes de prosseguir com a atualização. É prática recomendada também resolver avisos.

2. Clique em **seguinte**.
3. Clique em **Atualizar**.

   A validação é executada novamente. Quaisquer erros ou avisos restantes são apresentados juntamente com uma lista de ações corretivas. Os erros devem ser corrigidos antes de poder prosseguir com a atualização. Se a validação for concluída com avisos, corrija os avisos ou escolha **Atualizar com avisos**.

   > Por padrão, o ONTAP usa o "processo de atualização em lote" para atualizar clusters com oito ou mais nós. A partir do ONTAP 9.10,1, se preferir, você pode selecionar **Atualizar um par de HA de cada vez** para substituir o padrão e fazer com que o cluster atualize um par de HA de cada vez usando o processo de atualização contínua.

   Para configurações do MetroCluster com mais de 2 nós, o processo de atualização do ONTAP é iniciado simultaneamente nos pares de HA em ambos os locais. Para uma configuração de MetroCluster de 2 nós, a atualização é iniciada primeiro no site em que a atualização não é iniciada. A atualização no site restante começa após a primeira atualização estar completa.

4. Se a atualização parar devido a um erro, clique na mensagem de erro para visualizar os detalhes e corrija o erro e "retomar a atualização".

Depois de terminar

Depois que a atualização for concluída com êxito, o nó será reinicializado e você será redirecionado para a página de login do System Manager. Se o nó demorar muito tempo para reiniciar, você deve atualizar seu navegador.

CLI

1. Valide a imagem do software de destino do ONTAP

   > Se você estiver atualizando uma configuração do MetroCluster, primeiro execute as etapas a seguir no cluster A e execute as mesmas etapas no cluster B.

   a. Elimine o pacote de software ONTAP anterior:

   ```
   cluster image package delete -version <previous_ONTAP_Version>
   ```

   b. Carregue a imagem de software ONTAP de destino no repositório de pacotes do cluster:

   ```
   cluster image package get -url location
   ```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

Se você estiver executando um "atualização direta de multi-hop", você também precisará carregar o pacote de software para a versão intermediária do ONTAP necessária para sua atualização. Por exemplo, se você estiver atualizando do 9,8 para o 9.13.1, será necessário carregar o pacote de software para o ONTAP 9.12,1 e, em seguida, usar o mesmo comando para carregar o pacote de software para o 9.13.1.

c. Verifique se o pacote de software está disponível no repositório de pacotes de cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1             MM/DD/YYYY 10:32:15
```

d. Execute as verificações automatizadas de pré-atualização:

```
cluster image validate -version <package_version_number>
```

Se estiver executando um "atualização direta de multi-hop", você só precisará usar o pacote ONTAP de destino para verificação. Você não precisa validar a imagem de atualização intermediária separadamente. Por exemplo, se você estiver atualizando de 9,8 para 9.13.1, use o pacote 9.13.1 para verificação. Não é necessário validar o pacote 9.12.1 separadamente.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

a. Monitorize o progresso da validação:

```
cluster image show-update-progress
```

b. Conclua todas as ações necessárias identificadas pela validação.

c. Se você estiver atualizando uma configuração do MetroCluster, repita as etapas acima no cluster B.

2. Gerar uma estimativa de atualização de software:

```
cluster image update -version <package_version_number> -estimate
-only
```

> Se você estiver atualizando uma configuração do MetroCluster, poderá executar esse comando no cluster A ou no cluster B. não será necessário executá-lo em ambos os clusters.

A estimativa de atualização de software exibe detalhes sobre cada componente a ser atualizado, bem como a duração estimada da atualização.

3. Execute a atualização de software:

```
cluster image update -version <package_version_number>
```

- Se você estiver executando um "atualização direta de multi-hop", use a versão de destino do ONTAP para o package_version_number. Por exemplo, se você estiver atualizando do ONTAP 9.8 para 9.13.1, use 9.13.1 como o package_version_number.
- Por padrão, o ONTAP usa o "processo de atualização em lote" para atualizar clusters com oito ou mais nós. Se preferir, você pode usar o `-force-rolling` parâmetro para substituir o processo padrão e fazer com que o cluster atualize um nó de cada vez usando o processo de atualização contínua.
- Depois de concluir cada aquisição e giveback, a atualização aguarda 8 minutos para permitir que os aplicativos cliente se recuperem da pausa na e/S que ocorre durante a aquisição e a giveback. Se o seu ambiente exigir mais ou menos tempo para a estabilização do cliente, você pode usar o `-stabilize-minutes` parâmetro para especificar uma quantidade diferente de tempo de estabilização.
- Para configurações do MetroCluster com mais de 4 nós, a atualização automatizada começa simultaneamente nos pares de HA em ambos os locais. Para uma configuração de MetroCluster de 2 nós, a atualização é iniciada no site em que a atualização não é iniciada. A atualização no site restante começa após a primeira atualização estar completa.

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
--------------------- ----------
-----------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. Apresentar o progresso da atualização do cluster:

```
cluster image show-update-progress
```

Se você estiver atualizando uma configuração de MetroCluster de 4 nós ou 8 nós, o `cluster image show-update-progress` comando exibirá somente o progresso do nó no qual você executa o comando. Você deve executar o comando em cada nó para ver o progresso do nó individual.

5. Verifique se a atualização foi concluída com sucesso em cada nó.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

                                                 Estimated
Elapsed
Update Phase         Status                       Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                    00:10:00
00:02:07
Data ONTAP updates   completed                    01:31:00
01:39:00
Post-update checks   completed                    00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. Acione uma notificação AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Se o cluster não estiver configurado para enviar mensagens AutoSupport, uma cópia da notificação será salva localmente.

7. Se você estiver atualizando uma configuração de MetroCluster FC de 2 nós, verifique se o cluster está habilitado para switchover automático não planejado.

> Se você estiver atualizando uma configuração padrão, uma configuração MetroCluster IP ou uma configuração MetroCluster FC maior que 2 nós, não será necessário executar esta etapa.

a. Verifique se o switchover não planejado automático está ativado:

```
metrocluster show
```

Se o switchover não planejado automático estiver ativado, a seguinte instrução aparece na saída do comando:

```
AUSO Failure Domain    auso-on-cluster-disaster
```

a. Se a instrução não aparecer na saída, ative o switchover não planejado automático:

```
metrocluster modify -auto-switchover-failure-domain auso-on-
cluster-disaster
```

b. Verifique se o switchover não planejado automático foi ativado:

```
metrocluster show
```

Retomar a atualização do software ONTAP após um erro no processo de atualização automatizada

Se uma atualização automática do software ONTAP for interrompida devido a um erro, você deverá resolver o erro e continuar a atualização. Após o erro ser resolvido, você pode optar por continuar o processo de atualização automatizada ou concluir o processo de atualização manualmente. Se você optar por continuar a atualização automatizada, não execute nenhuma das etapas de atualização manualmente.

Exemplo 3. Passos

System Manager

1. Dependendo da versão do ONTAP que você está executando, execute uma das seguintes etapas:

Se você está correndo…	Então…
ONTAP 9 .8 ou posterior	Clique em **Cluster** > **Overview**
ONTAP 9.7, 9,6 ou 9,5	Clique em **Configuração** > **Cluster** > **Atualizar**.
ONTAP 9 .4 ou anterior	• Clique em **Configuração** > **Atualização de cluster**. • No canto direito do painel **Visão geral**, clique nos três pontos verticais azuis e selecione **Atualização do ONTAP**.

2. Continue a atualização automática ou cancele-a e continue manualmente.

Se você quiser…	Então…
Retomar a atualização automatizada	Clique em **Resume**.
Cancele a atualização automática e continue manualmente	Clique em **Cancelar**.

CLI

1. Veja o erro de atualização:

```
cluster image show-update-progress
```

2. Resolva o erro.
3. Retomar a atualização:

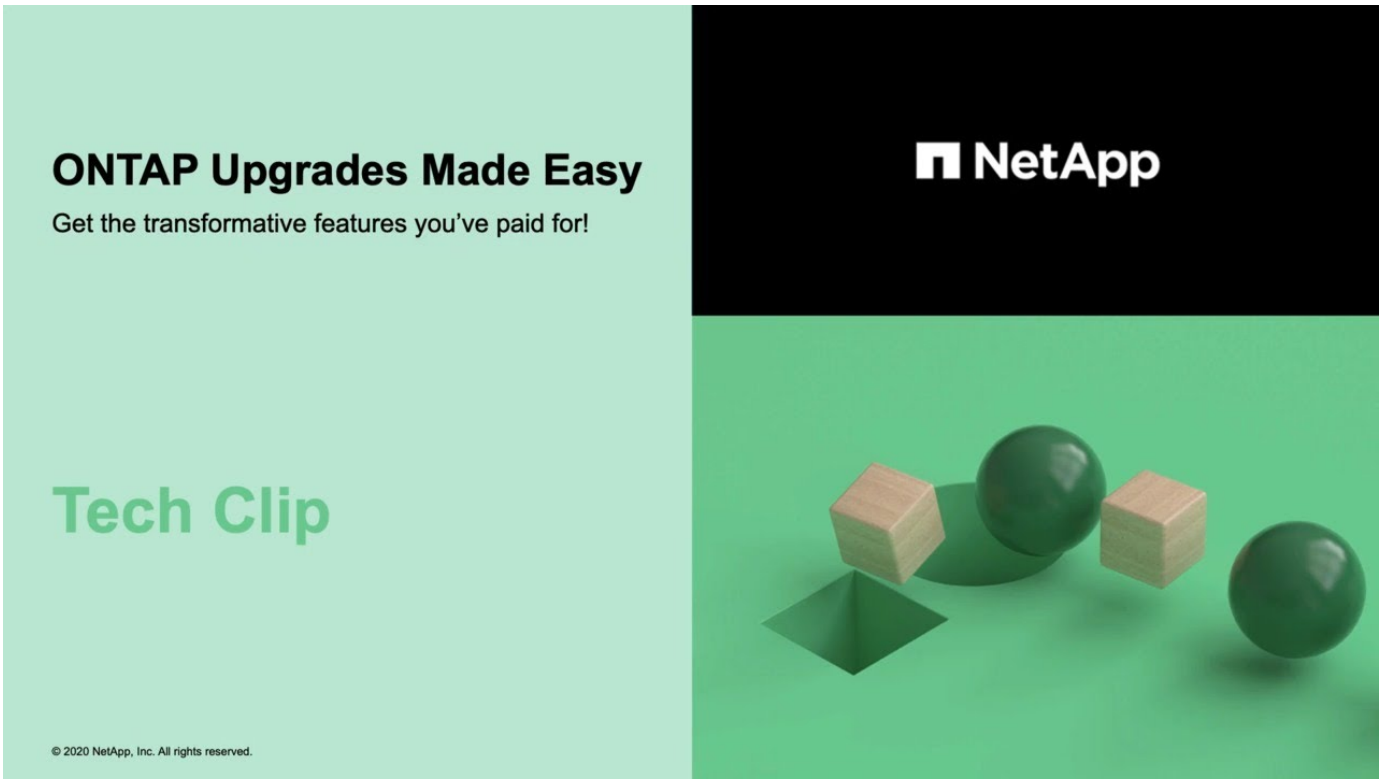
Se você quiser…	Digite o seguinte comando…
Retomar a atualização automatizada	`cluster image resume-update`
Cancele a atualização automática e continue manualmente	`cluster image cancel-update`

Depois de terminar

"Execute verificações pós-atualização".

Vídeo: Atualizações fáceis

Veja os recursos simplificados de atualização do ONTAP do System Manager no ONTAP 9.8.



Informações relacionadas

- "Inicie o consultor digital da Active IQ"
- "Documentação do consultor digital da Active IQ"

Atualizações manuais

Instale o pacote de software ONTAP para atualizações manuais

Depois de transferir o pacote de software ONTAP para uma atualização manual, tem de o instalar localmente antes de iniciar a atualização.

Passos

1. Defina o nível de privilégio como avançado, inserindo **y** quando solicitado a continuar: `set -privilege advanced`

   (`*>`É apresentado o aviso avançado).

2. Instale a imagem.

Se tiver a seguinte configuração…	Use este comando…
• Sem MetroCluster • MetroCluster de 2 nós	`system node image update -node * -package <location> -replace -package true -setdefault true -background true` `<location>` Pode ser um servidor Web ou uma pasta local, dependendo da versão do ONTAP. Consulte a `system node image update` página de manual para obter detalhes. Este comando instala a imagem do software em todos os nós simultaneamente. Para instalar a imagem em cada nó, uma de cada vez, não especifique o `-background` parâmetro.
• MetroCluster de 4 nós • Configuração de MetroCluster de 8 nós	`system node image update -node * -package <location> -replace -package true -background true -setdefault false` Você deve emitir este comando em ambos os clusters. Este comando usa uma consulta estendida para alterar a imagem do software de destino, que é instalada como a imagem alternativa em cada nó.

3. Digite `y` para continuar quando solicitado.
4. Verifique se a imagem do software está instalada em cada nó.

```
system node image show-update-progress -node *
```

Este comando exibe o status atual da instalação da imagem de software. Você deve continuar a executar este comando até que todos os nós relatem um **Status de execução** de **sair** e um **Status de saída** de **sucesso**.

O comando de atualização da imagem do nó do sistema pode falhar e apresentar mensagens de erro ou aviso. Depois de resolver quaisquer erros ou avisos, você pode executar o comando novamente.

Este exemplo mostra um cluster de dois nós no qual a imagem do software é instalada com sucesso em ambos os nós:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Atualização manual de ONTAP sem interrupções usando a CLI (configurações padrão)

A atualização automatizada usando o System Manager é o método de atualização preferido. Se o Gerenciador do sistema não oferecer suporte à sua configuração, você poderá usar a interface de linha de comando (CLI) do ONTAP para realizar uma atualização manual sem interrupções. Para atualizar um cluster de dois ou mais nós usando o método sem interrupções manual, você deve iniciar uma operação de failover em cada nó em um par de HA, atualizar o nó com falha, iniciar o giveback e repetir o processo para cada par de HA no cluster.

Antes de começar

Você precisa ter requisitos de atualização satisfeitos"preparação".

Atualizando o primeiro nó em um par de HA

Você pode atualizar o primeiro nó em um par de HA iniciando um takeover pelo parceiro do nó. O parceiro atende os dados do nó enquanto o primeiro nó é atualizado.

Se você estiver executando uma grande atualização, o primeiro nó a ser atualizado deve ser o mesmo nó no qual você configurou as LIFs de dados para conetividade externa e instalou a primeira imagem ONTAP.

Depois de atualizar o primeiro nó, você deve atualizar o nó do parceiro o mais rápido possível. Não permita que os dois nós permaneçam em um "versão mista" estado por mais tempo do que o necessário.

Passos

1. Atualize o primeiro nó no cluster invocando uma mensagem AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Esta notificação do AutoSupport inclui um registo do estado do sistema imediatamente antes da atualização. Ele salva informações úteis de solução de problemas no caso de haver um problema com o processo de atualização.

Se o cluster não estiver configurado para enviar mensagens AutoSupport, uma cópia da notificação será salva localmente.

2. Defina o nível de privilégio como avançado, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

(`*>`É apresentado o aviso avançado).

3. Defina a nova imagem do software ONTAP para ser a imagem padrão:

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

O comando System Image Modify (modificar imagem do sistema) usa uma consulta estendida para alterar a nova imagem do software ONTAP (que é instalada como imagem alternativa) para a imagem padrão do nó.

4. Monitorize o progresso da atualização:

```
system node upgrade-revert show
```

5. Verifique se a nova imagem do software ONTAP está definida como a imagem padrão:

```
system image show
```

No exemplo a seguir, image2 é a nova versão do ONTAP e é definida como a imagem padrão no node0:

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

6. Desative o giveback automático no nó do parceiro se estiver ativado:

```
storage failover modify -node nodenameB -auto-giveback false
```

Se o cluster for um cluster de dois nós, uma mensagem é exibida avisando que a desativação automática da giveback impede que os serviços do cluster de gerenciamento fiquem on-line em caso de falha alternada. Entre `y` para continuar.

7. Verifique se o giveback automático está desativado para o parceiro do nó:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. Execute o comando a seguir duas vezes para determinar se o nó a ser atualizado está atendendo a qualquer cliente no momento

```
system node run -node nodenameA -command uptime
```

O comando uptime exibe o número total de operações que o nó executou para clientes NFS, SMB, FC e iSCSI desde que o nó foi inicializado pela última vez. Para cada protocolo, você deve executar o comando duas vezes para determinar se as contagens de operação estão aumentando. Se eles estão aumentando, o nó está atendendo clientes para esse protocolo no momento. Se eles não estiverem aumentando, o nó não estará atendendo clientes para esse protocolo.

Você deve fazer uma nota de cada protocolo que tem operações de cliente crescentes para que, após o nó ser atualizado, você possa verificar se o tráfego de cliente foi retomado.

O exemplo a seguir mostra um nó com operações NFS, SMB, FC e iSCSI. No entanto, o nó está atualmente atendendo apenas clientes NFS e iSCSI.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Migre todos os LIFs de dados para fora do nó:

```
network interface migrate-all -node nodenameA
```

10. Verifique quaisquer LIFs que você migrou:

```
network interface show
```

Para obter mais informações sobre os parâmetros que você pode usar para verificar o status de LIF, consulte a página de manual da interface de rede show.

O exemplo a seguir mostra que LIFs de dados do node0 migraram com sucesso. Para cada LIF, os campos incluídos neste exemplo permitem verificar o nó e a porta inicial do LIF, o nó e a porta atuais para a qual o LIF migrou e o status operacional e administrativo do LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. Iniciar uma aquisição:

```
storage failover takeover -ofnode nodenameA
```

Não especifique o parâmetro -option immediate, porque um controle normal é necessário para o nó que está sendo levado para inicializar na nova imagem de software. Se você não migrar manualmente as LIFs para longe do nó, elas migrarão automaticamente para o parceiro de HA do nó para garantir que não haja interrupções no serviço.

O primeiro nó inicializa até o estado de espera para giveback.

> Se o AutoSupport estiver habilitado, uma mensagem AutoSupport será enviada indicando que o nó está fora do quórum do cluster. Pode ignorar esta notificação e prosseguir com a atualização.

12. Verifique se a aquisição foi bem-sucedida:

```
storage failover show
```

Você pode ver mensagens de erro indicando incompatibilidade de versão e problemas de formato da caixa postal. Esse é um comportamento esperado e representa um estado temporário em uma grande atualização sem interrupções e não é prejudicial.

O exemplo a seguir mostra que a aquisição foi bem-sucedida. O nó node0 está em espera para o estado de giveback, e seu parceiro está no estado de aquisição.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. Aguarde pelo menos oito minutos para que as seguintes condições entrem em vigor:
    - O multipathing do cliente (se implantado) está estabilizado.
    - Os clientes são recuperados da pausa em uma operação de e/S que ocorre durante a aquisição.

      O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

14. Retorne os agregados ao primeiro nó:

```
storage failover giveback -ofnode nodenameA
```

O giveback primeiro retorna o agregado raiz para o nó do parceiro e, depois que esse nó terminar a inicialização, retorna os agregados não-raiz e quaisquer LIFs que foram definidos para reverter automaticamente. O nó recém-inicializado começa a servir dados para clientes de cada agregado assim que o agregado é retornado.

15. Verifique se todos os agregados foram devolvidos:

```
storage failover show-giveback
```

Se o campo Status do Giveback indicar que não há agregados para devolver, todos os agregados foram retornados. Se o giveback for vetado, o comando exibirá o progresso da giveback e qual subsistema vetou a giveback.

16. Se algum agregado não tiver sido retornado, execute as seguintes etapas:
    a. Revise a solução alternativa de veto para determinar se você deseja abordar a condição "para" ou

substituir o veto.

b. Se necessário, aborde a condição "para" descrita na mensagem de erro, garantindo que todas as operações identificadas sejam terminadas graciosamente.

c. Execute novamente o comando Storage failover giveback.

   Se você decidiu substituir a condição "para", defina o parâmetro -override-vetos como true.

17. Aguarde pelo menos oito minutos para que as seguintes condições entrem em vigor:
    - O multipathing do cliente (se implantado) está estabilizado.
    - Os clientes são recuperados da pausa em uma operação de e/S que ocorre durante a giveback.

      O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

18. Verifique se a atualização foi concluída com sucesso para o nó:

    a. Vá para o nível de privilégio avançado :

    ```
    set -privilege advanced
    ```

    b. Verifique se o status da atualização está concluído para o nó:

    ```
    system node upgrade-revert show -node nodenameA
    ```

    O status deve ser listado como completo.

    Se o estado não estiver completo, contactar a assistência técnica.

    a. Voltar ao nível de privilégio de administrador:

    ```
    set -privilege admin
    ```

19. Verifique se as portas do nó estão ativas:

    ```
    network port show -node nodenameA
    ```

    Você deve executar este comando em um nó que é atualizado para a versão superior do ONTAP 9.

    O exemplo a seguir mostra que todas as portas do nó estão ativas:

```
cluster1::> network port show -node node0
                                                                        Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node0
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

20. Reverter os LIFs de volta para o nó:

```
network interface revert *
```

Este comando retorna os LIFs que foram migrados para longe do nó.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Verifique se as LIFs de dados do nó reverteram com êxito de volta para o nó e se eles estão ativos:

```
network interface show
```

O exemplo a seguir mostra que todas as LIFs de dados hospedadas pelo nó foram revertidas com êxito de volta para o nó e que seu status operacional está ativo:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0a
true
            data002      up/up    192.0.2.121/24     node0         e0b
true
            data003      up/up    192.0.2.122/24     node0         e0b
true
            data004      up/up    192.0.2.123/24     node0         e0a
true
4 entries were displayed.
```

22. Se você determinou anteriormente que esse nó serve clientes, verifique se o nó está fornecendo serviço para cada protocolo que ele estava fornecendo anteriormente:

```
system node run -node nodenameA -command uptime
```

As contagens de operação repostas para zero durante a atualização.

O exemplo a seguir mostra que o nó atualizado foi retomado servindo seus clientes NFS e iSCSI:

```
cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Reative o giveback automático no nó do parceiro se ele tiver sido desativado anteriormente:

```
storage failover modify -node nodenameB -auto-giveback true
```

Você deve continuar a atualizar o parceiro de HA do nó o mais rápido possível. Se você precisar suspender o processo de atualização por qualquer motivo, ambos os nós do par de HA deverão estar executando a mesma versão do ONTAP.

Atualizando o nó de parceiro em um par de HA

Depois de atualizar o primeiro nó em um par de HA, você atualiza o parceiro iniciando um takeover nele. O primeiro nó serve os dados do parceiro enquanto o nó do parceiro é atualizado.

1. Defina o nível de privilégio como avançado, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

(`*>`É apresentado o aviso avançado).

2. Defina a nova imagem do software ONTAP para ser a imagem padrão:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

O comando System Image Modify usa uma consulta estendida para alterar a nova imagem do software ONTAP (que é instalada como a imagem alternativa) para ser a imagem padrão do nó.

3. Monitorize o progresso da atualização:

```
system node upgrade-revert show
```

4. Verifique se a nova imagem do software ONTAP está definida como a imagem padrão:

```
system image show
```

No exemplo a seguir `image2`, está a nova versão do ONTAP e é definida como a imagem padrão no nó:

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

5. Desative o giveback automático no nó do parceiro se estiver ativado:

```
storage failover modify -node nodenameA -auto-giveback false
```

Se o cluster for um cluster de dois nós, uma mensagem é exibida avisando que a desativação automática da giveback impede que os serviços do cluster de gerenciamento fiquem on-line em caso de falha alternada. Entre `y` para continuar.

6. Verifique se o giveback automático está desativado para o nó do parceiro:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- -------------
node0    false
1 entry was displayed.
```

7. Execute o seguinte comando duas vezes para determinar se o nó a ser atualizado está atendendo a qualquer cliente no momento:

```
system node run -node nodenameB -command uptime
```

O comando uptime exibe o número total de operações que o nó executou para clientes NFS, SMB, FC e iSCSI desde que o nó foi inicializado pela última vez. Para cada protocolo, você deve executar o comando duas vezes para determinar se as contagens de operação estão aumentando. Se eles estão aumentando, o nó está atendendo clientes para esse protocolo no momento. Se eles não estiverem aumentando, o nó não estará atendendo clientes para esse protocolo.

Você deve fazer uma nota de cada protocolo que tem operações de cliente crescentes para que, após o nó ser atualizado, você possa verificar se o tráfego de cliente foi retomado.

O exemplo a seguir mostra um nó com operações NFS, SMB, FC e iSCSI. No entanto, o nó está atualmente atendendo apenas clientes NFS e iSCSI.

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migre todos os LIFs de dados para fora do nó:

```
network interface migrate-all -node nodenameB
```

9. Verifique o status de quaisquer LIFs que você migrou:

```
network interface show
```

Para obter mais informações sobre os parâmetros que você pode usar para verificar o status de LIF, consulte a página de manual da interface de rede show.

O exemplo a seguir mostra que LIFs de dados do node1 migraram com sucesso. Para cada LIF, os campos incluídos neste exemplo permitem verificar o nó e a porta inicial do LIF, o nó e a porta atuais para a qual o LIF migrou e o status operacional e administrativo do LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up          up
vs0     data002 node1     e0b       node0     e0b       up          up
vs0     data003 node1     e0b       node0     e0b       up          up
vs0     data004 node1     e0a       node0     e0a       up          up
4 entries were displayed.
```

10. Iniciar uma aquisição:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

Não especifique o parâmetro -option immediate, porque um controle normal é necessário para o nó que está sendo levado para inicializar na nova imagem de software. Se você não tiver migrado manualmente os LIFs para fora do nó, eles migrarão automaticamente para o parceiro de HA do nó para que não haja interrupções no serviço.

É apresentado um aviso. Tem de introduzir `y` para continuar.

O nó que é tomado sobre arranca até o estado de espera para giveback.

> Se o AutoSupport estiver habilitado, uma mensagem AutoSupport será enviada indicando que o nó está fora do quórum do cluster. Pode ignorar esta notificação e prosseguir com a atualização.

11. Verifique se a aquisição foi bem-sucedida:

```
storage failover show
```

O exemplo a seguir mostra que a aquisição foi bem-sucedida. O nó node1 está em espera para o estado

de giveback, e seu parceiro está no estado de aquisição.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. Aguarde pelo menos oito minutos para que as seguintes condições entrem em vigor
    - O multipathing do cliente (se implantado) está estabilizado.
    - Os clientes são recuperados da pausa na I/o que ocorre durante a aquisição.

      O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

13. Retorno dos agregados para o nó de parceiro:

    ```
    storage failover giveback -ofnode nodenameB
    ```

    A operação de giveback primeiro retorna o agregado raiz para o nó do parceiro e, depois que esse nó tiver terminado a inicialização, retorna os agregados não-raiz e quaisquer LIFs que foram definidos para reverter automaticamente. O nó recém-inicializado começa a servir dados para clientes de cada agregado assim que o agregado é retornado.

14. Verifique se todos os agregados são devolvidos:

    ```
    storage failover show-giveback
    ```

    Se o campo Status do Giveback indicar que não há agregados para devolver, todos os agregados serão retornados. Se o giveback for vetado, o comando exibirá o progresso da giveback e qual subsistema vetou a operação da giveback.

15. Se algum agregado não for retornado, execute as seguintes etapas:
    a. Revise a solução alternativa de veto para determinar se você deseja abordar a condição "para" ou substituir o veto.
    b. Se necessário, aborde a condição "para" descrita na mensagem de erro, garantindo que todas as operações identificadas sejam terminadas graciosamente.
    c. Execute novamente o comando Storage failover giveback.

       Se você decidiu substituir a condição "para", defina o parâmetro -override-vetos como true.

16. Aguarde pelo menos oito minutos para que as seguintes condições entrem em vigor:

- O multipathing do cliente (se implantado) está estabilizado.
- Os clientes são recuperados da pausa em uma operação de e/S que ocorre durante a giveback.

  O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

17. Verifique se a atualização foi concluída com sucesso para o nó:

    a. Vá para o nível de privilégio avançado :

    ```
    set -privilege advanced
    ```

    b. Verifique se o status da atualização está concluído para o nó:

    ```
    system node upgrade-revert show -node nodenameB
    ```

    O status deve ser listado como completo.

    Se o status não estiver concluído, a partir do nó, execute o `system node upgrade-revert upgrade` comando. Se o comando não concluir a atualização, entre em Contato com o suporte técnico.

    a. Voltar ao nível de privilégio de administrador:

    ```
    set -privilege admin
    ```

18. Verifique se as portas do nó estão ativas:

    ```
    network port show -node nodenameB
    ```

    Você deve executar este comando em um nó que foi atualizado para ONTAP 9.4.

    O exemplo a seguir mostra que todas as portas de dados do nó estão ativas:

```
cluster1::> network port show -node node1
                                                                   Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

19. Reverter os LIFs de volta para o nó:

```
network interface revert *
```

Este comando retorna os LIFs que foram migrados para longe do nó.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Verifique se as LIFs de dados do nó reverteram com êxito de volta para o nó e se eles estão ativos:

```
network interface show
```

O exemplo a seguir mostra que todas as LIFs de dados hospedadas pelo nó são revertidas com êxito de volta para o nó e que seu status operacional está ativo:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1         e0a
true
            data002      up/up    192.0.2.121/24     node1         e0b
true
            data003      up/up    192.0.2.122/24     node1         e0b
true
            data004      up/up    192.0.2.123/24     node1         e0a
true
4 entries were displayed.
```

21. Se você determinou anteriormente que esse nó serve clientes, verifique se o nó está fornecendo serviço para cada protocolo que ele estava fornecendo anteriormente:

```
system node run -node nodenameB -command uptime
```

As contagens de operação repostas para zero durante a atualização.

O exemplo a seguir mostra que o nó atualizado foi retomado servindo seus clientes NFS e iSCSI:

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. Se este foi o último nó no cluster a ser atualizado, acione uma notificação do AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Esta notificação do AutoSupport inclui um registo do estado do sistema imediatamente antes da atualização. Ele salva informações úteis de solução de problemas no caso de haver um problema com o processo de atualização.

Se o cluster não estiver configurado para enviar mensagens AutoSupport, uma cópia da notificação será salva localmente.

23. Confirme se o novo software ONTAP está em execução em ambos os nós do par de HA:

```
set -privilege advanced
```

```
system node image show
```

No exemplo a seguir, image2 é a versão atualizada do ONTAP e é a versão padrão em ambos os nós:

```
cluster1::*> system node image show
                 Is      Is                Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. Reative o giveback automático no nó do parceiro se ele tiver sido desativado anteriormente:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Verifique se o cluster está no quórum e se os serviços estão sendo executados usando os `cluster show` comandos e `cluster ring show` (nível avançado de privilégio).

    Você deve executar esta etapa antes de atualizar quaisquer pares de HA adicionais.

26. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

27. Atualizar quaisquer pares de HA adicionais.

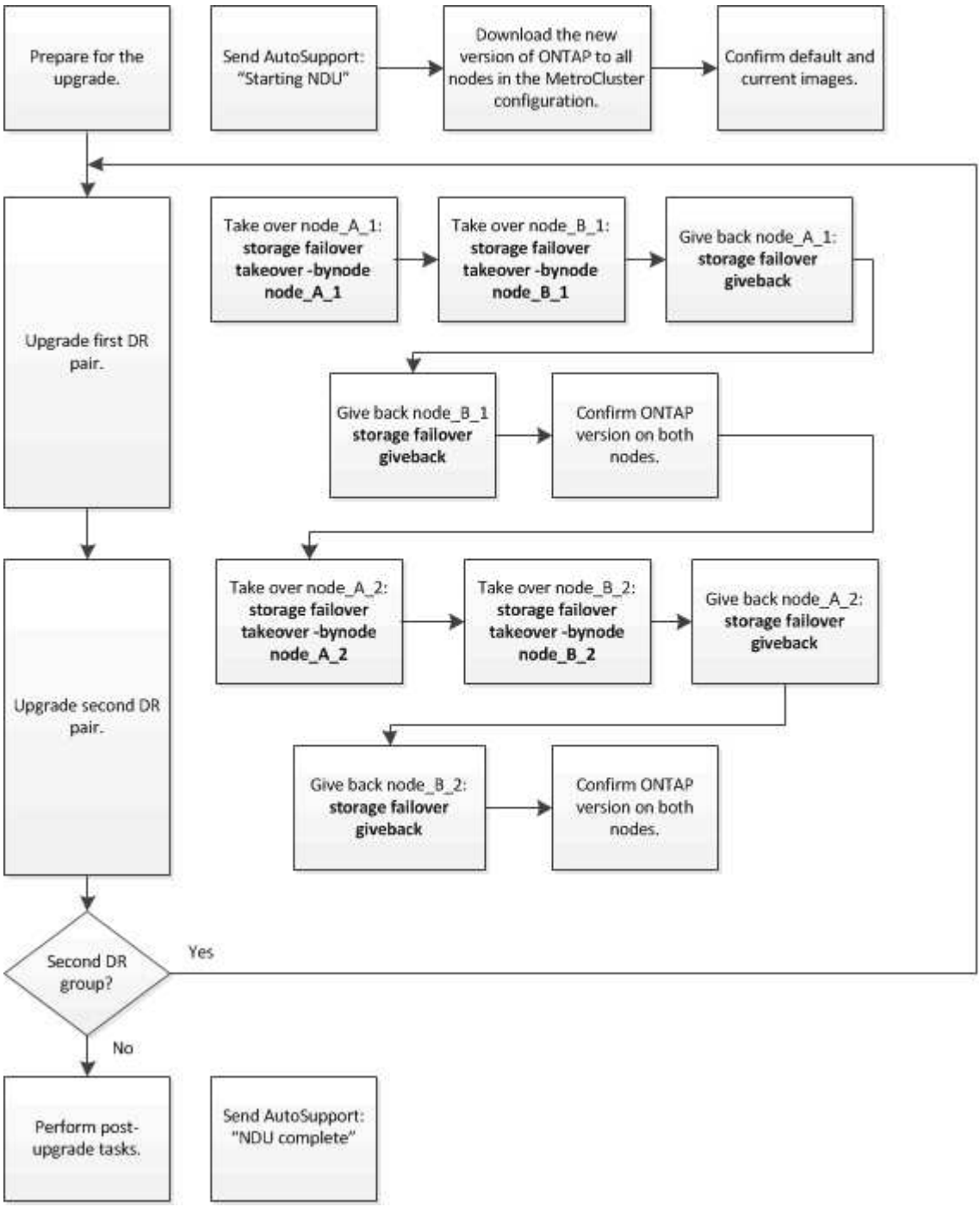
Atualização manual de ONTAP sem interrupções de uma configuração de MetroCluster de quatro ou oito nós usando a CLI

Uma atualização manual de uma configuração do MetroCluster de quatro ou oito nós envolve a preparação para a atualização, a atualização dos pares de DR em cada um dos um ou dois grupos de DR simultaneamente e a execução de tarefas pós-atualização.

- Esta tarefa aplica-se às seguintes configurações:
  - Configurações IP ou FC MetroCluster de quatro nós executando o ONTAP 9.2 ou anterior

- Configurações de FC MetroCluster de oito nós, independentemente da versão do ONTAP

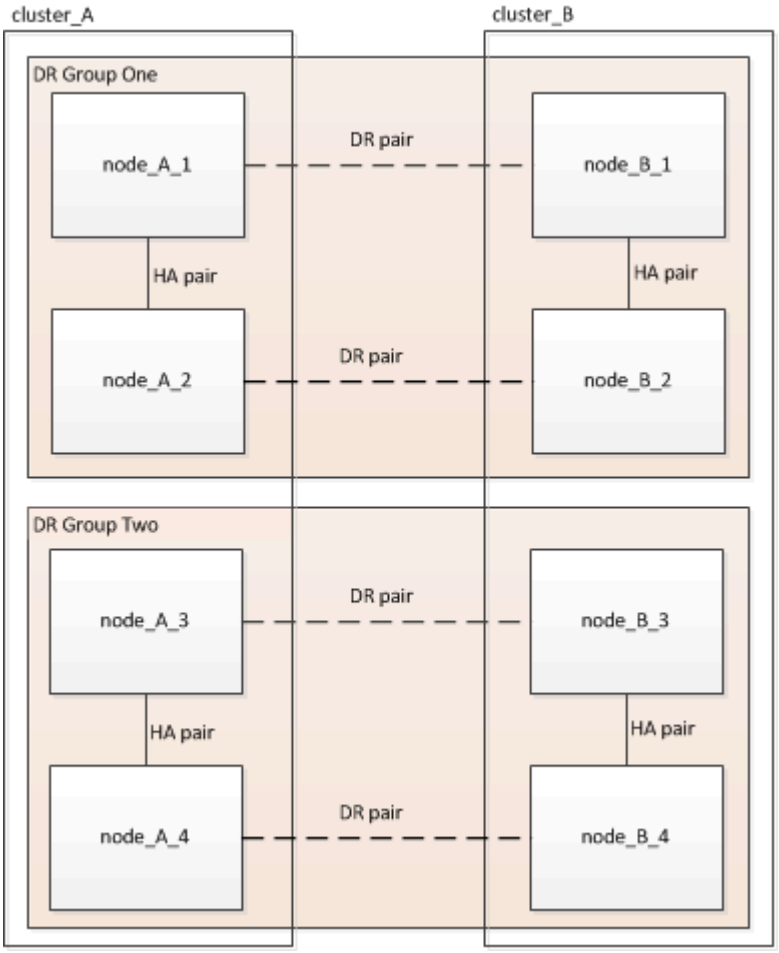
- Se você tiver uma configuração de MetroCluster de dois nós, não use este procedimento.
- As seguintes tarefas referem-se às versões antigas e novas do ONTAP.
  - Ao atualizar, a versão antiga é uma versão anterior do ONTAP, com um número de versão menor do que a nova versão do ONTAP.
  - Ao fazer o downgrade, a versão antiga é uma versão posterior do ONTAP, com um número de versão maior do que a nova versão do ONTAP.
- Esta tarefa utiliza o seguinte fluxo de trabalho de alto nível:



Diferenças ao atualizar o software ONTAP em uma configuração de MetroCluster de oito ou quatro nós

O processo de atualização do software MetroCluster difere, dependendo se há oito ou quatro nós na configuração do MetroCluster.

Uma configuração do MetroCluster consiste em um ou dois grupos de DR. Cada grupo de DR consiste em dois pares de HA, um par de HA em cada cluster do MetroCluster. Um MetroCluster de oito nós inclui dois grupos de DR:



Você atualiza um grupo de DR de cada vez.

Para configurações de MetroCluster de quatro nós:

1. Atualizar o grupo de RD 1:
   a. Atualize node_A_1 e node_B_1.
   b. Atualize node_A_2 e node_B_2.

Para configurações de MetroCluster de oito nós, você executa o procedimento de atualização do grupo de DR duas vezes:

1. Atualizar o grupo de RD 1:
   a. Atualize node_A_1 e node_B_1.
   b. Atualize node_A_2 e node_B_2.
2. Atualizar Grupo DR dois:
   a. Atualize node_A_3 e node_B_3.

b. Atualize node_A_4 e node_B_4.

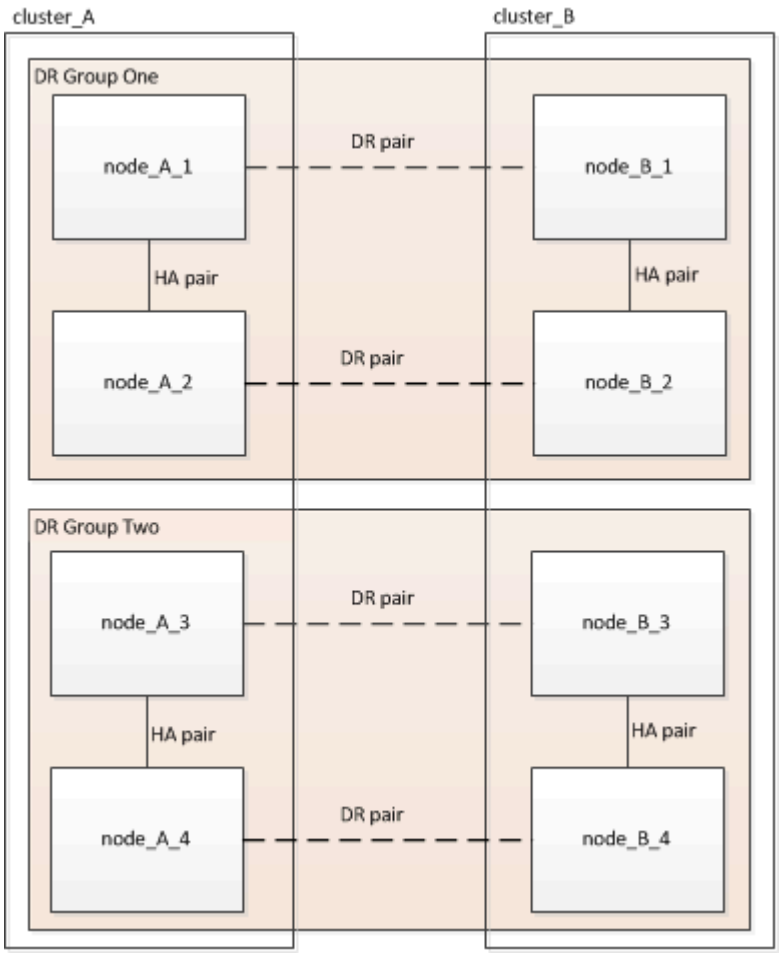
Preparando-se para atualizar um grupo de DR do MetroCluster

Antes de atualizar o software ONTAP nos nós, você deve identificar as relações de DR entre os nós, enviar uma mensagem do AutoSupport informando que você está iniciando uma atualização e confirmar a versão do ONTAP em execução em cada nó.

Você deve ter "transferido" e "instalado" as imagens de software.

Essa tarefa deve ser repetida em cada grupo de DR. Se a configuração do MetroCluster consistir em oito nós, haverá dois grupos de DR. Assim, essa tarefa deve ser repetida em cada grupo de DR.

Os exemplos fornecidos nesta tarefa usam os nomes mostrados na ilustração a seguir para identificar os clusters e nós:



1. Identifique os pares de DR na configuração:

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
4 entries were displayed.

cluster_A::>
```

2. Defina o nível de privilégio de admin para Advanced, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

(`*>`É apresentado o aviso avançado).

3. Confirme a versão do ONTAP no cluster_A:

```
system image show
```

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- -------   -------------------
node_A_1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Confirme a versão no cluster_B:

```
system image show
```

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- -------     -------------------
node_B_1
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node_B_2
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. Acione uma notificação AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Esta notificação do AutoSupport inclui um registo do estado do sistema antes da atualização. Ele salva informações úteis de solução de problemas se houver um problema com o processo de atualização.

Se o cluster não estiver configurado para enviar mensagens AutoSupport, uma cópia da notificação será salva localmente.

6. Para cada nó no primeiro conjunto, defina a imagem do software ONTAP de destino como a imagem padrão:

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

Este comando usa uma consulta estendida para alterar a imagem do software de destino, que é instalada como imagem alternativa, para ser a imagem padrão para o nó.

7. Verifique se a imagem do software ONTAP de destino está definida como a imagem padrão no cluster_A:

```
system image show
```

No exemplo a seguir, image2 é a nova versão do ONTAP e é definida como a imagem padrão em cada um dos nós no primeiro conjunto:

```
cluster_A::*> system image show
                  Is      Is              Install
Node     Image    Default Current Version Date
-------- -------  ------- ------- ------- -------------------
node_A_1
         image1   false   true    X.X.X   MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y   MM/DD/YYYY TIME
node_A_2
         image1   false   true    X.X.X   MM/DD/YYYY TIME
         image2   true   false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

a. Verifique se a imagem do software ONTAP de destino está definida como a imagem padrão no cluster_B:

```
system image show
```

O exemplo a seguir mostra que a versão de destino é definida como a imagem padrão em cada um dos nós no primeiro conjunto:

```
cluster_B::*> system image show
                  Is      Is              Install
Node     Image    Default Current Version Date
-------- -------  ------- ------- ------- -------------------
node_A_1
         image1   false   true    X.X.X   MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y   MM/YY/YYYY TIME
node_A_2
         image1   false   true    X.X.X   MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

8. Determine se os nós a serem atualizados estão atendendo a clientes duas vezes para cada nó:

```
system node run -node target-node -command uptime
```

O comando uptime exibe o número total de operações que o nó executou para clientes NFS, CIFS, FC e iSCSI desde que o nó foi inicializado pela última vez. Para cada protocolo, você precisa executar o comando duas vezes para determinar se as contagens de operação estão aumentando. Se eles estão aumentando, o nó está atendendo clientes para esse protocolo no momento. Se eles não estiverem aumentando, o nó não estará atendendo clientes para esse protocolo.

Você deve fazer uma nota de cada protocolo que tem operações de cliente crescentes para que, após o nó ser atualizado, você possa verificar se o tráfego de cliente foi retomado.

Este exemplo mostra um nó com operações NFS, CIFS, FC e iSCSI. No entanto, o nó está atualmente atendendo apenas clientes NFS e iSCSI.

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Atualizando o primeiro par de DR em um grupo de DR do MetroCluster

Você precisa executar um takeover e giveback dos nós na ordem correta para fazer da nova versão do ONTAP a versão atual do nó.

Todos os nós devem estar executando a versão antiga do ONTAP.

Nesta tarefa, node_A_1 e node_B_1 são atualizados.

Se você atualizou o software ONTAP no primeiro grupo DR e está atualizando o segundo grupo DR em uma configuração de MetroCluster de oito nós, nesta tarefa você estaria atualizando node_A_3 e node_B_3.

1. Se o software tiebreaker do MetroCluster estiver ativado, desabilite-o.
2. Para cada nó no par de HA, desative a opção giveback automática:

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   Esse comando deve ser repetido para cada nó no par de HA.

3. Verifique se a giveback automática está desativada:

   ```
   storage failover show -fields auto-giveback
   ```

   Este exemplo mostra que o giveback automático foi desativado em ambos os nós:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 false
node_x_2 false
2 entries were displayed.
```

4. Certifique-se de que a e/S não exceda os aproximadamente 50% para cada controladora e que a utilização de CPU não exceda os aproximadamente 50% por controladora.
5. Inicie um takeover do nó de destino no cluster_A:

   Não especifique o parâmetro -option immediate, porque um controle normal é necessário para os nós que estão sendo levados para inicializar na nova imagem de software.

   a. Assuma o parceiro DR no cluster_A (node_a_1):

      ```
      storage failover takeover -ofnode node_A_1
      ```

      O nó inicializa até o estado "aguardando pela giveback".

      > Se o AutoSupport estiver ativado, uma mensagem AutoSupport será enviada indicando que os nós estão fora do quórum do cluster. Você pode ignorar esta notificação e prosseguir com a atualização.

   b. Verifique se a aquisição foi bem-sucedida:

      ```
      storage failover show
      ```

      O exemplo a seguir mostra que a aquisição foi bem-sucedida. Node_A_1 está no estado "aguardando giveback" e node_A_2 está no estado "na aquisição".

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       -        Waiting for giveback (HA
mailboxes)
node_A_2       node_A_1       false    In takeover
2 entries were displayed.
```

6. Assuma o parceiro DR no cluster_B (node_B_1):

   Não especifique o parâmetro -option immediate, porque um controle normal é necessário para os nós que

estão sendo levados para inicializar na nova imagem de software.

a. Assumir node_B_1:

```
storage failover takeover -ofnode node_B_1
```

O nó inicializa até o estado "aguardando pela giveback".

> Se o AutoSupport estiver ativado, uma mensagem AutoSupport será enviada indicando que os nós estão fora do quórum do cluster. Você pode ignorar esta notificação e prosseguir com a atualização.

b. Verifique se a aquisição foi bem-sucedida:

```
storage failover show
```

O exemplo a seguir mostra que a aquisição foi bem-sucedida. Node_B_1 está no estado "aguardando giveback" e node_B_2 está no estado "em aquisição".

```
 cluster1::> storage failover show
                                Takeover
 Node           Partner        Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
 node_B_2       node_B_1       false    In takeover
 2 entries were displayed.
```

7. Aguarde pelo menos oito minutos para garantir as seguintes condições:
   - O multipathing do cliente (se implantado) está estabilizado.
   - Os clientes são recuperados da pausa na I/o que ocorre durante a aquisição.

     O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

8. Retornar os agregados aos nós de destino:

   Depois de atualizar as configurações IP do MetroCluster para o ONTAP 9.5 ou posterior, os agregados ficarão em estado degradado por um curto período antes da ressincronização e retorno a um estado espelhado.

   a. Devolver os agregados ao parceiro de DR no cluster_A:

```
storage failover giveback -ofnode node_A_1
```

b. Devolver os agregados ao parceiro de DR no cluster_B:

```
storage failover giveback -ofnode node_B_1
```

A operação giveback primeiro retorna o agregado raiz para o nó e, depois que o nó terminar de inicializar, retorna os agregados não-raiz.

9. Verifique se todos os agregados foram retornados emitindo o seguinte comando em ambos os clusters:

```
storage failover show-giveback
```

Se o campo Status do Giveback indicar que não há agregados para devolver, todos os agregados foram retornados. Se o giveback for vetado, o comando exibirá o progresso da giveback e qual subsistema vetou a giveback.

10. Se algum agregado não tiver sido devolvido, faça o seguinte:
    a. Revise a solução alternativa de veto para determinar se você deseja abordar a condição "para" ou substituir o veto.
    b. Se necessário, aborde a condição "para" descrita na mensagem de erro, garantindo que todas as operações identificadas sejam terminadas graciosamente.
    c. Reinsira o comando Storage failover giveback.

    Se você decidiu substituir a condição "para", defina o parâmetro -override-vetos como true.

11. Aguarde pelo menos oito minutos para garantir as seguintes condições:
    ◦ O multipathing do cliente (se implantado) está estabilizado.
    ◦ Os clientes são recuperados da pausa em I/o que ocorre durante a giveback.

    O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

12. Defina o nível de privilégio de admin para Advanced, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

(`*>`É apresentado o aviso avançado).

13. Confirme a versão no cluster_A:

```
system image show
```

O exemplo a seguir mostra que o sistema image2 deve ser a versão padrão e atual no node_A_1:

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------  ------------------
node_A_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

14. Confirme a versão no cluster_B:

```
system image show
```

O exemplo a seguir mostra que o sistema image2 (ONTAP 9.0,0) é a versão padrão e atual no node_A_1:

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------  ------------------
node_B_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_B_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

Atualizando o segundo par de DR em um grupo de DR do MetroCluster

Você precisa executar um takeover e giveback do nó na ordem correta para fazer da nova versão do ONTAP a versão atual do nó.

Você deve ter atualizado o primeiro par de DR (node_A_1 e node_B_1).

Nesta tarefa, node_A_2 e node_B_2 são atualizados.

Se você atualizou o software ONTAP no primeiro grupo de DR e está atualizando o segundo grupo de DR em uma configuração de MetroCluster de oito nós, nesta tarefa você está atualizando node_A_4 e node_B_4.

1. Migre todos os LIFs de dados para fora do nó:

```
network interface migrate-all -node nodenameA
```

2. Inicie um takeover do nó de destino no cluster_A:

   Não especifique o parâmetro -option immediate, porque um controle normal é necessário para os nós que estão sendo levados para inicializar na nova imagem de software.

   a. Assuma o controle do parceiro DR no cluster_A:

```
storage failover takeover -ofnode node_A_2 -option allow-version-
mismatch
```

   > A `allow-version-mismatch` opção não é necessária para atualizações do ONTAP 9.0 para o ONTAP 9.1 ou para quaisquer atualizações de patch.

   O nó inicializa até o estado "aguardando pela giveback".

   Se o AutoSupport estiver ativado, uma mensagem AutoSupport será enviada indicando que os nós estão fora do quórum do cluster. Você pode ignorar esta notificação e prosseguir com a atualização.

   b. Verifique se a aquisição foi bem-sucedida:

```
storage failover show
```

   O exemplo a seguir mostra que a aquisição foi bem-sucedida. Node_A_2 está no estado "aguardando giveback" e node_A_1 está no estado "na aquisição".

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. Inicie um takeover do nó de destino no cluster_B:

   Não especifique o parâmetro -option immediate, porque um controle normal é necessário para os nós que estão sendo levados para inicializar na nova imagem de software.

   a. Assuma o parceiro DR no cluster_B (node_B_2):

Se você está atualizando de…	Digite este comando…
ONTAP 9.2 ou ONTAP 9.1	`storage failover takeover -ofnode node_B_2`
ONTAP 9 .0 ou Data ONTAP 8.3.x	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` A `allow-version-mismatch` opção não é necessária para atualizações do ONTAP 9.0 para o ONTAP 9.1 ou para quaisquer atualizações de patch.

O nó inicializa até o estado "aguardando pela giveback".

Se o AutoSupport estiver habilitado, uma mensagem AutoSupport será enviada indicando que os nós estão fora do quórum do cluster. Você pode ignorar esta notificação com segurança e prosseguir com a atualização.

b. Verifique se a aquisição foi bem-sucedida:

```
storage failover show
```

O exemplo a seguir mostra que a aquisição foi bem-sucedida. Node_B_2 está no estado "aguardando giveback" e node_B_1 está no estado "em aquisição".

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. Aguarde pelo menos oito minutos para garantir as seguintes condições:
   - O multipathing do cliente (se implantado) está estabilizado.
   - Os clientes são recuperados da pausa na I/o que ocorre durante a aquisição.

O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

5. Retornar os agregados aos nós de destino:

   Depois de atualizar as configurações IP do MetroCluster para o ONTAP 9.5, os agregados estarão em um estado degradado por um curto período antes da ressincronização e retorno a um estado espelhado.

   a. Devolver os agregados ao parceiro de DR no cluster_A:

      ```
      storage failover giveback -ofnode node_A_2
      ```

   b. Devolver os agregados ao parceiro de DR no cluster_B:

      ```
      storage failover giveback -ofnode node_B_2
      ```

      A operação giveback primeiro retorna o agregado raiz para o nó e, depois que o nó terminar de inicializar, retorna os agregados não-raiz.

6. Verifique se todos os agregados foram retornados emitindo o seguinte comando em ambos os clusters:

   ```
   storage failover show-giveback
   ```

   Se o campo Status do Giveback indicar que não há agregados para devolver, todos os agregados foram retornados. Se o giveback for vetado, o comando exibirá o progresso da giveback e qual subsistema vetou a giveback.

7. Se algum agregado não tiver sido devolvido, faça o seguinte:
   a. Revise a solução alternativa de veto para determinar se você deseja abordar a condição "para" ou substituir o veto.
   b. Se necessário, aborde a condição "para" descrita na mensagem de erro, garantindo que todas as operações identificadas sejam terminadas graciosamente.
   c. Reinsira o comando Storage failover giveback.

      Se você decidiu substituir a condição "para", defina o parâmetro -override-vetos como true.

8. Aguarde pelo menos oito minutos para garantir as seguintes condições:
   - O multipathing do cliente (se implantado) está estabilizado.
   - Os clientes são recuperados da pausa em I/o que ocorre durante a giveback.

     O tempo de recuperação é específico do cliente e pode demorar mais de oito minutos, dependendo das caraterísticas dos aplicativos cliente.

9. Defina o nível de privilégio de admin para Advanced, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

(`*>`É apresentado o aviso avançado).

10. Confirme a versão no cluster_A:

```
system image show
```

O exemplo a seguir mostra que o sistema image2 (imagem ONTAP de destino) é a versão padrão e atual no node_A_2:

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_A_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_A_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. Confirme a versão no cluster_B:

```
system image show
```

O exemplo a seguir mostra que o sistema image2 (imagem ONTAP de destino) é a versão padrão e atual no node_B_2:

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_B_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_B_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

12. Para cada nó no par de HA, habilite a giveback automática:

```
storage failover modify -node target-node -auto-giveback true
```

Esse comando deve ser repetido para cada nó no par de HA.

13. Verifique se o giveback automático está ativado:

```
storage failover show -fields auto-giveback
```

Este exemplo mostra que o giveback automático foi ativado em ambos os nós:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

Atualização sem interrupções de uma configuração de MetroCluster de dois nós no ONTAP 9.2 ou anterior

A forma como você atualiza uma configuração do MetroCluster de dois nós varia de acordo com a versão do ONTAP. Se você estiver executando o ONTAP 9.2 ou anterior, use este procedimento para executar uma atualização sem interrupções manual, que inclui iniciar um switchover negociado, atualizar o cluster no local com falha, iniciar o switchback e repetir o processo no cluster no outro local.

Se você tiver uma configuração de MetroCluster de dois nós executando o ONTAP 9.3 ou posterior, execute um Atualização automatizada usando o System Manager.

Passos

1. Defina o nível de privilégio como avançado, inserindo **y** quando solicitado a continuar:

```
set -privilege advanced
```

(`*>`É apresentado o aviso avançado).

2. No cluster a ser atualizado, instale a nova imagem do software ONTAP como padrão:

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. Verifique se a imagem do software de destino está definida como a imagem padrão:

```
system node image show
```

O exemplo a seguir mostra que `NewImage` está definido como a imagem padrão:

```
cluster_B::*> system node image show
                     Is      Is                            Install
Node     Image       Default Current Version               Date
-------- -------     ------- ------- --------------------
-------------------
node_B_1
         OldImage  false   true    X.X.X                 MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                 MM/DD/YYYY TIME
2 entries were displayed.
```

4. Se a imagem do software de destino não estiver definida como a imagem padrão, altere-a:

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Verifique se todos os SVMs do cluster estão em um estado de integridade:

```
metrocluster vserver show
```

6. No cluster que não está sendo atualizado, inicie um switchover negociado:

```
metrocluster switchover
```

A operação pode demorar vários minutos. Você pode usar o comando MetroCluster Operation show para verificar se o switchover foi concluído.

No exemplo a seguir, um switchover negociado é executado no cluster remoto ("'cluster_A'"). Isso faz com que o cluster local ("'cluster_B') pare para que você possa atualizá-lo.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Verifique se todos os SVMs do cluster estão em um estado de integridade:

```
metrocluster vserver show
```

8. Ressincronizar os agregados de dados no cluster "URVIVING":

```
metrocluster heal -phase aggregates
```

Depois de atualizar as configurações IP do MetroCluster para o ONTAP 9.5 ou posterior, os agregados ficarão em estado degradado por um curto período antes da ressincronização e retorno a um estado espelhado.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Verifique se a operação de recuperação foi concluída com sucesso:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Ressincronizar os agregados de raiz no cluster "URVIVING":

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Verifique se a operação de recuperação foi concluída com sucesso:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. No cluster interrompido, inicie o nó a partir do prompt Loader:

```
boot_ontap
```

13. Aguarde até que o processo de inicialização seja concluído e verifique se todos os SVMs de cluster estão em um estado de integridade:

```
metrocluster vserver show
```

14. Execute um switchback do cluster "URVIving":

```
metrocluster switchback
```

15. Verifique se o switchback foi concluído com sucesso:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Verifique se todos os SVMs do cluster estão em um estado de integridade:

```
metrocluster vserver show
```

17. Repita todas as etapas anteriores no outro cluster.
18. Verifique se a configuração do MetroCluster está em bom estado:
    a. Verificar a configuração:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

    b. Se você quiser ver resultados mais detalhados, use o comando MetroCluster check run:

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

    c. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

d. Simule a operação de comutação:

```
metrocluster switchover -simulate
```

e. Reveja os resultados da simulação de comutação:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

g. Repita essas subetapas no outro cluster.

Depois de terminar

Execute qualquer "tarefas pós-atualização".

Informações relacionadas

"Recuperação de desastres da MetroCluster"

Atualização manual do ONTAP disruptiva usando a CLI

Se você puder colocar o cluster off-line para atualizar para uma nova versão do ONTAP, poderá usar o método de atualização disruptiva. Este método tem várias etapas: Desativar o failover de armazenamento para cada par de HA, reinicializar cada nó no cluster e, em seguida, reativar o failover de armazenamento.

- Você deve "transferir" e "instale" a imagem do software.
- Se você estiver operando em um ambiente SAN, todos os clientes SAN devem ser desligados ou suspensos até que a atualização seja concluída.

  Se os clientes SAN não forem desligados ou suspensos antes de uma atualização disruptiva , os sistemas de arquivos e aplicativos do cliente sofrerão erros que podem exigir recuperação manual após a conclusão da atualização.

Em uma atualização disruptiva, o tempo de inatividade é necessário porque o failover de storage é desativado para cada par de HA e cada nó é atualizado. Quando o failover de storage é desativado, cada nó se comporta como um cluster de nó único; ou seja, os serviços de sistema associados ao nó são interrompidos pelo tempo que o sistema for reinicializado.

Passos

1. Defina o nível de privilégio de admin para Advanced, inserindo **y** quando solicitado a continuar:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

2. Defina a nova imagem do software ONTAP para ser a imagem padrão:

   ```
   system image modify {-node * -iscurrent false} -isdefault true
   ```

   Este comando usa uma consulta estendida para alterar a imagem do software ONTAP de destino (que é instalada como a imagem alternativa) para ser a imagem padrão para cada nó.

3. Verifique se a nova imagem do software ONTAP está definida como a imagem padrão:

   ```
   system image show
   ```

   No exemplo a seguir, a imagem 2 é a nova versão do ONTAP e é definida como a imagem padrão em ambos os nós:

   ```
   cluster1::*> system image show
                    Is      Is                Install
   Node     Image   Default Current Version    Date
   -------- ------- ------- ------- --------- -------------------
   node0
            image1  false   true    X.X.X     MM/DD/YYYY TIME
            image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
   node1
            image1  false   true    X.X.X     MM/DD/YYYY TIME
            image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
   4 entries were displayed.
   ```

4. Execute uma das seguintes etapas:

Se o cluster consistir em…	Faça isso…
Um nó	Avance para o passo seguinte.

Se o cluster consistir em…	Faça isso…

Dois nós	a. Desativar a alta disponibilidade do cluster:
	`cluster ha modify -configured false`
	Digite `y` para continuar quando solicitado.
	b. Desativar o failover de armazenamento para o par de HA:
	`storage failover modify -node * -enabled false`

Mais de dois nós	Desative o failover de storage para cada par de HA no cluster: `storage failover modify -node * -enabled false`

5. Reinicie um nó no cluster:

```
system node reboot -node nodename -ignore-quorum-warnings
```

Não reinicie mais de um nó de cada vez.

O nó inicializa a nova imagem ONTAP. O prompt de login do ONTAP é exibido, indicando que o processo de reinicialização está concluído.

6. Após o nó ou conjunto de nós reiniciar com a nova imagem ONTAP, defina o nível de privilégio como avançado:

```
set -privilege advanced
```

Digite **y** quando solicitado a continuar

7. Confirme se o novo software está em execução:

```
system node image show
```

No exemplo a seguir, image1 é a nova versão do ONTAP e é definida como a versão atual no node0:

```
cluster1::*> system node image show
                  Is      Is                    Install
Node     Image    Default Current Version       Date
-------- -------  ------- ------- --------      -------------------
node0
         image1   true    true    X.X.X          MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y         MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X         MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y         MM/DD/YYYY TIME
4 entries were displayed.
```

8. Verifique se a atualização foi concluída com sucesso:

   a. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

   b. Verifique se o status da atualização está concluído para cada nó:

   ```
   system node upgrade-revert show -node nodename
   ```

   O status deve ser listado como completo.

   Se o estado não estiver concluído, "Entre em Contato com o suporte da NetApp"imediatamente.

   a. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

9. Repita as etapas de 2 a 8 para cada nó adicional.
10. Se o cluster consistir em dois ou mais nós, ative o failover de storage para cada par de HA no cluster:

```
storage failover modify -node * -enabled true
```

11. Se o cluster consistir em apenas dois nós, ative a alta disponibilidade do cluster:

```
cluster ha modify -configured true
```

O que fazer após uma atualização do ONTAP

O que fazer após uma atualização do ONTAP

Depois de atualizar o ONTAP, há várias tarefas que você deve executar para verificar a prontidão do cluster.

1. "Verifique o cluster".

   Depois de atualizar o ONTAP, verifique a versão do cluster, a integridade do cluster e a integridade do storage. Se você estiver usando uma configuração MetroCluster FC, também precisará verificar se o cluster está habilitado para switchover automático não planejado.

2. "Verifique se todos os LIFs estão em portas residenciais".

   Durante uma reinicialização, alguns LIFs podem ter sido migrados para suas portas de failover atribuídas. Depois de atualizar um cluster, você deve habilitar e reverter quaisquer LIFs que não estejam em suas portas iniciais.

3. Verifique "considerações especiais" específico para o cluster.

   Se existirem determinadas configurações no cluster, poderá ser necessário executar passos adicionais após a atualização.

4. "Atualizar o Pacote de Qualificação de disco (DQP)".

   O DQP não é atualizado como parte de uma atualização do ONTAP.

Verifique o cluster após a atualização do ONTAP

Depois de atualizar o ONTAP, verifique a versão do cluster, a integridade do cluster e a integridade do storage. Para configurações do MetroCluster FC, verifique também se o cluster está habilitado para switchover automático não planejado.

Verifique a versão do cluster

Depois que todos os pares de HA tiverem sido atualizados, use o comando version para verificar se todos os nós estão executando a liberação de destino.

A versão do cluster é a versão mais baixa do ONTAP em execução em qualquer nó no cluster. Se a versão do cluster não for a versão de destino do ONTAP, você poderá atualizar o cluster.

1. Verifique se a versão do cluster é a versão de destino do ONTAP:

   ```
   version
   ```

2. Se a versão do cluster não for a versão de destino do ONTAP, você deve verificar o status de atualização de todos os nós:

   ```
   system node upgrade-revert show
   ```

Verifique a integridade do cluster

Depois de atualizar um cluster, você deve verificar se os nós estão íntegros e qualificados para participar do cluster e se o cluster está em quórum.

1. Verifique se os nós do cluster estão online e estão qualificados para participar do cluster:

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

Se algum nó não for saudável ou não for elegível, verifique se há erros nos logs do EMS e tome medidas corretivas.

2. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

3. Verifique os detalhes de configuração para cada processo RDB.

   - A época do banco de dados relacional e as epochs do banco de dados devem corresponder para cada nó.
   - O mestre de quórum por anel deve ser o mesmo para todos os nós.

     Observe que cada anel pode ter um mestre de quórum diferente.

Para exibir este processo RDB…	Digite este comando…
Aplicação de gerenciamento	`cluster ring show -unitname mgmt`
Base de dados de localização de volume	`cluster ring show -unitname vldb`
Gerenciador de interface virtual	`cluster ring show -unitname vifmgr`
Daemon de gerenciamento SAN	`cluster ring show -unitname bcomd`

     Este exemplo mostra o processo do banco de dados de localização de volume:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Se você estiver operando em um ambiente SAN, verifique se cada nó está em um quórum de SAN:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

Informações relacionadas

"Administração do sistema"

Verificar se o switchover não planejado automático está ativado (somente configurações MetroCluster FC)

Se o seu cluster estiver em uma configuração MetroCluster FC, você deve verificar se o switchover automático não planejado está ativado depois de atualizar o ONTAP.

Se estiver a utilizar uma configuração IP do MetroCluster, ignore este procedimento.

Passos

1. Verifique se o switchover não planejado automático está ativado:

```
metrocluster show
```

Se o switchover não planejado automático estiver ativado, a seguinte instrução aparece na saída do comando:

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. Se a instrução não aparecer, ative um switchover não planejado automático:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

3. Verifique se um switchover não planejado automático foi ativado:

```
metrocluster show
```

Informações relacionadas

"Gerenciamento de disco e agregado"

Verifique se todos os LIFS estão em portas domésticas após a atualização do ONTAP

Durante a reinicialização que ocorre como parte do processo de atualização do ONTAP, alguns LIFs podem ser migrados de suas portas domésticas para suas portas de failover atribuídas. Após uma atualização, você precisa ativar e reverter quaisquer LIFs que não estejam em suas portas domésticas.

Passos

1. Apresentar o estado de todas as LIFs:

```
network interface show -fields home-port,curr-port
```

Se **Status Admin** estiver "inativo" ou **for home** for "false" para quaisquer LIFs, continue com a próxima etapa.

2. Ativar os LIFs de dados:

```
network interface modify {-role data} -status-admin up
```

3. Reverter LIFs para suas portas domésticas:

```
network interface revert *
```

4. Verifique se todos os LIFs estão em suas portas residenciais:

```
network interface show
```

Este exemplo mostra que todos os LIFs para SVM vs0 estão em suas portas domésticas.

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network          Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node     Port    Home
-------- ---------- ---------- ---------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24   node0    e0e     true
         data002    up/up      192.0.2.121/24   node0    e0f     true
         data003    up/up      192.0.2.122/24   node0    e2a     true
         data004    up/up      192.0.2.123/24   node0    e2b     true
         data005    up/up      192.0.2.124/24   node1    e0e     true
         data006    up/up      192.0.2.125/24   node1    e0f     true
         data007    up/up      192.0.2.126/24   node1    e2a     true
         data008    up/up      192.0.2.127/24   node1    e2b     true
8 entries were displayed.
```

Configurações especiais

Considerações especiais após uma atualização do ONTAP

Se o cluster estiver configurado com qualquer um dos seguintes recursos, talvez seja necessário executar etapas adicionais depois de atualizar o software ONTAP.

Pergunte a si mesmo…	Se a sua resposta for sim, então faça isso…
Eu atualizei do ONTAP 9.7 ou anterior para o ONTAP 9.8 ou posterior?	Verifique a configuração da rede Remova o serviço EMS LIF das políticas de serviço de rede que não fornecem alcance para o destino EMS
Meu cluster está em uma configuração do MetroCluster?	Verifique o status da rede e do armazenamento
Tenho uma configuração SAN?	Verifique a configuração da SAN
Eu atualizei do ONTAP 9.3 ou anterior e estou usando o NetApp Storage Encryption?	Reconfigure as conexões do servidor KMIP
Tenho espelhos de partilha de carga?	Relocate os volumes de origem do espelho de compartilhamento de carga movidos
Tenho contas de usuário para acesso ao processador de Serviço (SP) criadas antes do ONTAP 9.9,1?	Verifique a alteração nas contas que podem acessar o processador de serviço

Verifique a configuração da rede após uma atualização do ONTAP a partir do ONTAP 9.7x ou anterior

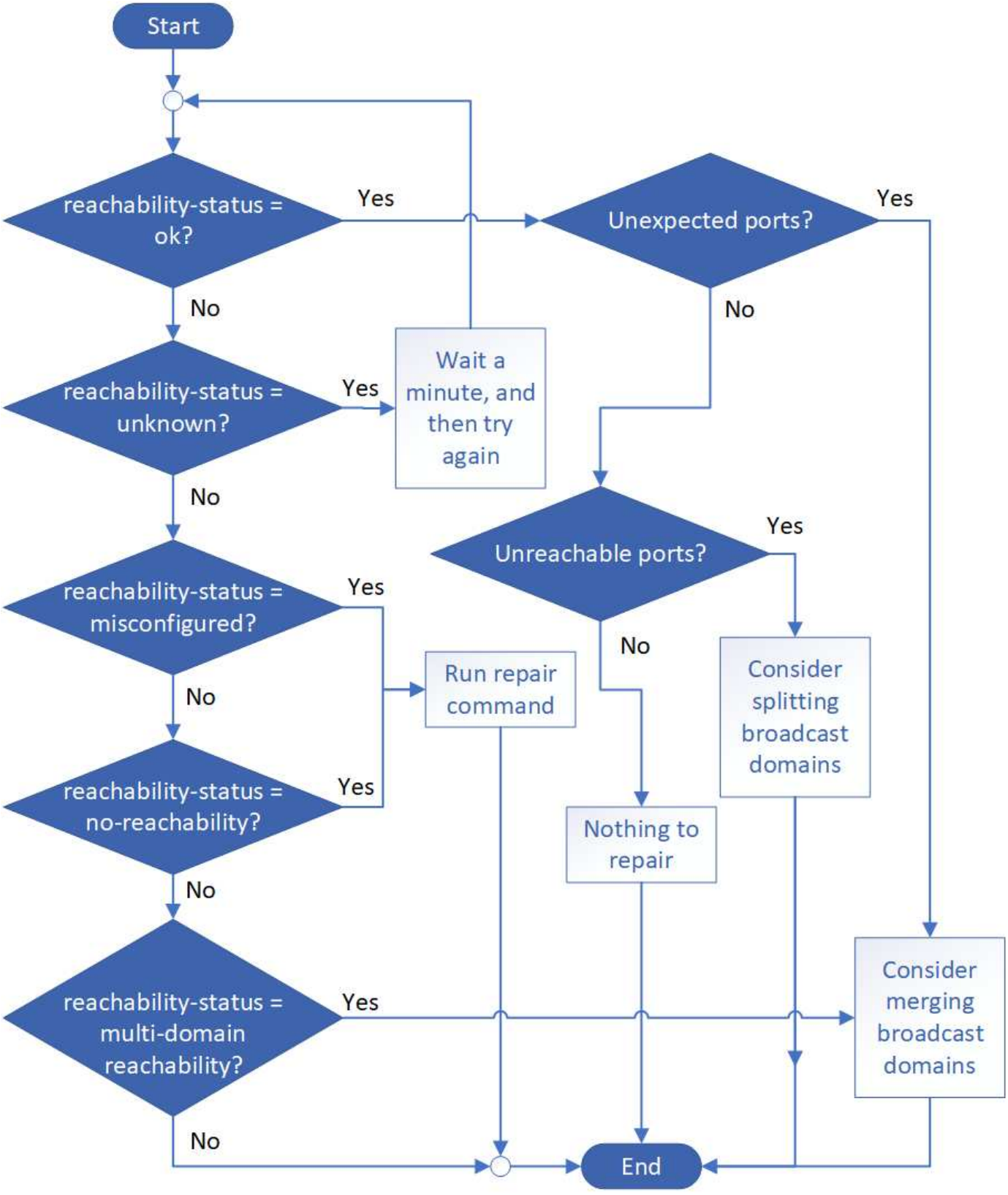
Depois de atualizar do ONTAP 9.7x ou anterior para o ONTAP 9.8 ou posterior, verifique a configuração da rede. Após a atualização, o ONTAP monitora automaticamente a acessibilidade da camada 2.

Passo

1. Verifique se cada porta tem acessibilidade ao domínio de broadcast esperado:

```
network port reachability show -detail
```

O comando output contém resultados de acessibilidade. Use a seguinte árvore de decisão e tabela para entender os resultados de acessibilidade (status de acessibilidade) e determinar o que, se houver, fazer a seguir.



status de acessibilidade	Descrição

ok	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído. Se o status de acessibilidade for "ok", mas houver "portas inesperadas", considere mesclar um ou mais domínios de broadcast. Para obter mais informações, "Mesclar domínios de broadcast"consulte . Se o status de acessibilidade for "ok", mas houver "portas inalcançáveis", considere dividir um ou mais domínios de broadcast. Para obter mais informações, "Dividir domínios de broadcast"consulte . Se o status de acessibilidade for "ok" e não houver portas inesperadas ou inacessíveis, sua configuração está correta.
acessibilidade mal configurada	A porta não tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, a porta tem acessibilidade da camada 2 para um domínio de broadcast diferente. Você pode reparar a acessibilidade da porta. Ao executar o seguinte comando, o sistema atribuirá a porta ao domínio de broadcast ao qual tem acessibilidade: `network port reachability repair -node -port` Para obter mais informações, "Acessibilidade da porta de reparo"consulte .
sem acessibilidade	A porta não tem acessibilidade da camada 2 para qualquer domínio de broadcast existente. Você pode reparar a acessibilidade da porta. Quando você executa o seguinte comando, o sistema atribuirá a porta a um novo domínio de broadcast criado automaticamente no IPspace padrão: `network port reachability repair -node -port` Para obter mais informações, "Acessibilidade da porta de reparo"consulte .
multidomínio-acessibilidade	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast. Examine a conetividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast. Para obter mais informações, consulte "Mesclar domínios de broadcast" ou "Acessibilidade da porta de reparo".
desconhecido	Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.

Depois de reparar uma porta, você precisa verificar e resolver LIFs e VLANs deslocados. Se a porta fazia parte de um grupo de interfaces, você também precisa entender o que aconteceu com esse grupo de interfaces. Para obter mais informações, "Acessibilidade da porta de reparo"consulte .

Remova o serviço EMS LIF das políticas de serviço de rede

Se você tiver mensagens do sistema de gerenciamento de eventos (EMS) configuradas antes de atualizar do ONTAP 9.7 ou anterior para o ONTAP 9.8 ou posterior , após a atualização, as mensagens do EMS podem não ser entregues.

Durante a atualização, o Management-ems, que é o serviço EMS LIF, é adicionado a todas as políticas de serviço existentes. Isso permite que mensagens EMS sejam enviadas de qualquer uma das LIFs associadas a qualquer uma das políticas de serviço. Se o LIF selecionado não tiver acessibilidade ao destino de notificação de eventos, a mensagem não será entregue.

Para evitar isso, após a atualização, você deve remover o serviço EMS LIF das políticas de serviço de rede que não fornecem acessibilidade ao destino.

Passos

1. Identificar as LIFs e as políticas de serviço de rede associadas através das quais as mensagens EMS podem ser enviadas:

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------ ------------------
cluster-1      cluster_mgmt
                                    default-management
cluster-1      node1-mgmt
                                    default-management
cluster-1      node2-mgmt
                                    default-management
cluster-1      inter_cluster
                                    default-intercluster
4 entries were displayed.
```

2. Verifique se cada LIF tem conetividade com o destino EMS:

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

   Execute isso em cada nó.

Exemplos

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Introduzir nível de privilégio avançado:

```
set advanced
```

4. Para os LIFs que não têm acessibilidade, remova o serviço Management-ems LIF das políticas de serviço correspondentes:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

5. Verifique se o LIF de gestão-ems está agora associado apenas aos LIFs que fornecem acessibilidade ao destino EMS:

```
network interface show -fields service-policy -services management-ems
```

Links relacionados

"LIFs e políticas de serviço no ONTAP 9.6 e posteriores"

Verifique o status de rede e armazenamento para configurações do MetroCluster após uma atualização do ONTAP

Depois de atualizar um cluster ONTAP em uma configuração do MetroCluster, verifique o status das LIFs, agregados e volumes para cada cluster.

1. Verifique o status de LIF:

```
network interface show
```

Em operação normal, os LIFs para SVMs de origem devem ter um status de administrador de up e estar localizados em seus nós de origem. Os LIFs para SVMs de destino não precisam estar ativos ou localizados em seus nós de origem. No switchover, todos os LIFs têm um status de administrador de up, mas eles não precisam estar localizados em seus nós domésticos.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

2. Verifique o estado dos agregados:

```
storage aggregate show -state !online
```

Este comando exibe todos os agregados que estão *não* online. Em operação normal, todos os agregados localizados no local devem estar on-line. No entanto, se a configuração do MetroCluster estiver em switchover, os agregados de raiz no local de recuperação de desastres podem estar offline.

Este exemplo mostra um cluster em funcionamento normal:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

Este exemplo mostra um cluster em switchover, no qual os agregados raiz no local de recuperação de

desastres estão offline:

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. Verifique o estado dos volumes:

```
volume show -state !online
```

Este comando exibe todos os volumes que estão *não* online.

Se a configuração do MetroCluster estiver em operação normal (ela não estiver no estado de switchover), a saída deverá mostrar todos os volumes pertencentes aos SVMs secundárias do cluster (aqueles com o nome SVM anexado a "-mc").

Esses volumes só estão online em caso de mudança.

Este exemplo mostra um cluster em operação normal, no qual os volumes no local de recuperação de desastres não estão online.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. Verifique se não existem volumes inconsistentes:

```
volume show -is-inconsistent true
```

Consulte o artigo da base de dados de Conhecimento "Volume Mostrando WAFL inconsistente"sobre como resolver os volumes inconsistentes.

Verifique a configuração da SAN após uma atualização

Após uma atualização do ONTAP, em um ambiente SAN, você deve verificar se cada iniciador que foi conetado a um LIF antes da atualização foi reconetado com êxito ao LIF.

1. Verifique se cada iniciador está conetado ao LIF correto.

   Você deve comparar a lista de iniciadores com a lista que você fez durante a preparação da atualização. Se você estiver executando o ONTAP 9.11,1 ou posterior, use o Gerenciador do sistema para exibir o status da conexão, pois ele oferece uma exibição muito mais clara do que a CLI.

System Manager

a. No System Manager, clique em **hosts > SAN Initiator Groups**.

   A página exibe uma lista de grupos de iniciadores (grupos de iniciadores). Se a lista for grande, você pode visualizar páginas adicionais da lista clicando nos números de página no canto inferior direito da página.

   As colunas exibem várias informações sobre os grupos. A partir de 9.11.1, o estado da ligação do grupo também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

CLI

- Listar iniciadores iSCSI:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- Listar iniciadores FC:

```
fcp initiator show -fields igroup,wwpn,lif
```

Reconfigure as conexões do servidor KMIP após uma atualização do ONTAP 9.2 ou anterior

Depois de atualizar do ONTAP 9.2 ou anterior para o ONTAP 9.3 ou posterior, você precisa reconfigurar todas as conexões de servidor de gerenciamento de chaves externas (KMIP).

Passos

1. Configurar a conetividade do gerenciador de chaves:

```
security key-manager setup
```

2. Adicione seus servidores KMIP:

```
security key-manager add -address <key_management_server_ip_address>
```

3. Verifique se os servidores KMIP estão conetados:

```
security key-manager show -status
```

4. Consultar os servidores-chave:

```
security key-manager query
```

5. Crie uma nova chave de autenticação e frase-passe:

```
security key-manager create-key -prompt-for-key true
```

A frase-passe tem de ter um mínimo de 32 carateres.

6. Consultar a nova chave de autenticação:

```
security key-manager query
```

7. Atribua a nova chave de autenticação aos seus discos de encriptação automática (SEDs):

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```

Certifique-se de que está a utilizar a nova chave de autenticação da sua consulta.

8. Se necessário, atribua uma chave FIPS às SEDs:

```
storage encryption disk modify -disk <disk_id> -fips-key-id
<fips_authentication_key_id>
```

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

Relocate os volumes de origem de espelho de compartilhamento de carga movidos após uma atualização do ONTAP

Depois de atualizar o ONTAP, você precisa mover os volumes de origem de espelhamento de compartilhamento de carga de volta para os locais de pré-atualização.

Passos

1. Identifique o local para o qual você está movendo o volume de origem do espelho de compartilhamento de carga usando o Registro que você criou antes de mover o volume de origem do espelho de compartilhamento de carga.
2. Mova o volume de origem do espelho de compartilhamento de carga de volta para sua localização original:

```
volume move start
```

Alteração nas contas de usuário que podem acessar o processador de serviço

Se você criou contas de usuário no ONTAP 9.8 ou anterior que possam acessar o processador de serviço (SP) com uma função não admin e atualizar para o ONTAP 9.9,1 ou posterior, qualquer valor não admin no `-role` parâmetro será modificado para `admin`.

Para obter mais informações, "Contas que podem acessar o SP"consulte .

Atualize o Pacote de Qualificação de disco

Depois de atualizar seu software ONTAP, você deve baixar e instalar o Pacote de Qualificação de disco do ONTAP (DQP). O DQP não é atualizado como parte de uma atualização do ONTAP.

O DQP contém os parâmetros adequados para a interação ONTAP com todas as unidades recém-qualificadas. Se a sua versão do DQP não contiver informações para uma unidade recém-qualificada, o ONTAP não terá as informações para configurar corretamente a unidade.

É prática recomendada atualizar o DQP a cada trimestre. Você também deve atualizar o DQP pelas seguintes razões:

- Sempre que você adicionar um novo tipo ou tamanho de unidade a um nó no cluster

  Por exemplo, se você já tiver unidades de 1 TB e adicionar unidades de 2 TB, precisará verificar a atualização DQP mais recente.

- Sempre que atualizar o firmware do disco
- Sempre que estiverem disponíveis ficheiros DQP ou firmware de disco mais recentes

Informações relacionadas

- "NetApp Downloads: Pacote de Qualificação de disco"
- "Downloads do NetApp: Firmware da unidade de disco"

Atualizações de firmware, sistema e segurança

Visão geral das atualizações de firmware, sistema e segurança

Dependendo da sua versão do ONTAP, você pode ativar atualizações automáticas de firmware, sistema e segurança.

Versão de ONTAP	O que está incluído nas atualizações automáticas
9.16.1 e mais tarde	• Proteção autônoma contra ransomware com inteligência artificial (ARP/AI) • Base de dados de Fuso horário do ONTAP • Firmware de storage para dispositivos de storage, discos e compartimentos de disco • Firmware SP/BMC para processadores de serviço e módulos BMC

Versão de ONTAP	O que está incluído nas atualizações automáticas
9.13.1 e mais tarde	• Base de dados de Fuso horário do ONTAP • Firmware de storage para dispositivos de storage, discos e compartimentos de disco • Firmware SP/BMC para processadores de serviço e módulos BMC
9.10.1 e mais tarde	• Firmware de storage para dispositivos de storage, discos e compartimentos de disco • Firmware SP/BMC para processadores de serviço e módulos BMC
9.9.1 e anteriores	Não suportado

Se uma atualização automática não estiver disponível para a sua versão do ONTAP ou se não tiver atualizações automáticas ativadas, pode executar atualizações de firmware, base de dados de fuso horário e segurança manualmente.

Links relacionados

- "Aprenda a fazer atualizações de firmware manualmente"
- "artigo da Knowledge base, como atualizar informações de fuso horário no ONTAP 9"
- "Aprenda a fazer atualizações de segurança manualmente"

Vídeo: Recurso de atualização automática de firmware

Veja o recurso de atualização automática de firmware disponível a partir do ONTAP 9.10,1.

Como as atualizações automáticas são agendadas para instalação

Todos os nós qualificados dentro do mesmo cluster são agrupados para atualizações automáticas. O período de tempo em que os nós elegíveis são agendados para atualização automática varia de acordo com o nível de prioridade da atualização e a porcentagem de sistemas em seu ambiente que exigem a atualização.

Por exemplo, se 10% ou menos do total de seus sistemas forem elegíveis para uma atualização não prioritária, a atualização será agendada para todos os sistemas elegíveis dentro de 1 semana. No entanto, se 76% ou mais do total de seus sistemas forem elegíveis para uma atualização não prioritária, a atualização será escalonada nos sistemas elegíveis ao longo de 8 semanas. Essa instalação escalonada ajuda a reduzir riscos para o seu ambiente geral se houver um problema com uma atualização que precise ser remediada.

A porcentagem do total de sistemas programados para atualizações automáticas por semana é a seguinte:

Para atualizações críticas

% dos sistemas que necessitam de atualização	% de atualizações que ocorrem na semana 1	% de atualizações que ocorrem na semana 2
50% ou menos	100%	
50-100%	30%	70%

Para atualizações de alta prioridade

% dos sistemas que necessitam de atualização	% de atualizações que ocorrem por semana			
	semana 1	**semana 2**	**semana 3**	**semana 4**
25% ou menos	100%			
26-50%	30%	70%		
50-100%	10%	20%	30%	40%

Para atualizações de prioridade normal

% dos sistemas que necessitam de atualização	% de atualizações que ocorrem por semana							
	semana 1	**semana 2**	**semana 3**	**semana 4**	**semana 5**	**semana 6**	**semana 7**	**semana 8**
10% ou menos	100%							
11-20%	30%	70%						
21-50%	10%	20%	30%	40%				

% dos sistemas que necessitam de atualização	% de atualizações que ocorrem por semana							
51-75%	5%	10%	15%	20%	20%	30%		
76-100%	5%	5%	10%	10%	15%	15%	20%	20%

Ativar atualizações automáticas

Ativar atualizações automáticas permite que o ONTAP baixe e instale atualizações de firmware, sistema e segurança sem a sua intervenção.

A disponibilidade de atualizações automáticas varia de acordo com a sua versão do ONTAP.

Versão de ONTAP	Atualizações automáticas disponíveis	Habilitado por padrão para…
9.16.1 e mais tarde	• Proteção autônoma contra ransomware com inteligência artificial (ARP/AI) • Base de dados de Fuso horário do ONTAP • Firmware de storage para dispositivos de storage, discos e compartimentos de disco • Firmware SP/BMC para processadores de serviço e módulos BMC	Mostrar notificações
9.13.1 e mais tarde	• Base de dados de Fuso horário do ONTAP • Firmware de storage para dispositivos de storage, discos e compartimentos de disco • Firmware SP/BMC para processadores de serviço e módulos BMC	Atualizar automaticamente
9.10.1 e mais tarde	• Firmware de storage para dispositivos de storage, discos e compartimentos de disco • Firmware SP/BMC para processadores de serviço e módulos BMC	Atualizar automaticamente

Antes de começar

- Você precisa ter um direito de suporte atual. Isso pode ser validado na "Site de suporte da NetApp"página **Detalhes do sistema**.
- Para ativar as atualizações automáticas, você deve primeiro ativar o AutoSupport com HTTPS. Se o AutoSupport não estiver ativado no cluster ou se o AutoSupport estiver ativado no cluster com outro protocolo de transporte, terá a opção de ativá-lo com HTTPS durante este procedimento.

O AutoSupport OnDemand é ativado por padrão e funcional quando configurado para enviar mensagens para suporte técnico usando o protocolo de transporte HTTPS.

Sobre esta tarefa

Dependendo da sua versão do ONTAP, as configurações padrão na página **Ativar atualizações automáticas** para arquivos de firmware, sistema ou segurança serão definidas para atualizar automaticamente ou mostrar notificações. Certifique-se de que confirma que estas definições estão corretas para o seu ambiente antes de concluir o procedimento específico da versão adequado.

Exemplo 4. Passos

ONTAP 9.16,1 e posterior

1. No System Manager, navegue até **Cluster > Settings**.
2. Se não tiver o AutoSupport OnDemand ativado com HTTPS, clique em para ativar as definições necessárias para prosseguir.
3. Na seção **atualizações de software**, clique em **Ativar**.
4. Especifique a ação a ser tomada para cada tipo de atualização.

   Você pode optar por atualizar automaticamente, mostrar notificações ou ignorar automaticamente as atualizações para cada tipo de atualização.

5. Aceite os termos e condições e selecione **Guardar**.

ONTAP 9.15,1 e anteriores

1. No System Manager, clique em **Eventos**.
2. Na seção **Visão geral**, ao lado de **Ativar atualização automática**, clique em **ações > Ativar**.
3. Se você não tiver o AutoSupport com HTTPS habilitado, selecione-o para ativá-lo.
4. Aceite os termos e condições e selecione **Guardar**.

Informações relacionadas

- "Prepare-se para usar o AutoSupport"
- "Solucionar problemas de entrega de mensagens AutoSupport em HTTP ou HTTPS"

Modificar atualizações automáticas

Quando as atualizações automáticas estão ativadas, por predefinição, o ONTAP deteta, transfere e instala automaticamente todas as atualizações recomendadas. Se você quiser ver as atualizações recomendadas antes de serem instaladas ou se quiser que as recomendações sejam descartadas automaticamente, você pode modificar o comportamento padrão de acordo com sua preferência.

Exemplo 5. Passos

ONTAP 9.16,1 e posterior

1. No System Manager, navegue até **Cluster > Settings**.
2. Na seção **atualizações de software**, → selecione .
3. Selecione a guia **todas as outras atualizações** e clique em **Editar configurações de atualização automática**.
4. Especifique as ações padrão a serem executadas para cada tipo de atualização.

   Você pode optar por atualizar automaticamente, mostrar notificações ou ignorar automaticamente as atualizações para cada tipo de atualização.

   ⓘ A base de dados de Fuso horário do ONTAP é controlada pelo tipo de atualização **arquivos do sistema**.

5. Aceite os termos e condições e selecione **Guardar**.

ONTAP 9.15,1 e anteriores

1. No System Manager, clique em **Cluster > Settings**.
2. Na seção **Atualização automática**, clique ⋮ para exibir uma lista de ações.
3. Clique em **Edit Automatic Update Settings** (Editar definições de atualização automática).
4. Especifique as ações padrão a serem executadas para cada tipo de atualização.

   Você pode optar por atualizar automaticamente, mostrar notificações ou ignorar automaticamente as atualizações para cada tipo.

   ⓘ A base de dados de Fuso horário do ONTAP é controlada pelo tipo de atualização DOS FICHEIROS DE SISTEMA.

Gerenciar atualizações automáticas recomendadas

O log de atualização automática exibe uma lista de recomendações de atualização e detalhes sobre cada um, incluindo uma descrição, categoria, horário programado para instalação, status e quaisquer erros. Você pode visualizar o log e, em seguida, decidir que ação você gostaria de executar para cada recomendação.

Passos

1. Veja a lista de recomendações:

Ver a partir das definições de cluster	Ver a partir do separador Update (Atualização)
a. Clique em **Cluster > Settings**. b. Siga um destes procedimentos, dependendo da sua versão do ONTAP: ◦ Para o ONTAP 9.15,1 e versões anteriores, na seção **Atualização automática**, clique em e, em seguida, clique na opção para exibir todas as atualizações. ◦ Para ONTAP 9.16,1 e posterior, na seção **atualizações de software**, selecione . No canto direito do painel **todas as outras atualizações**, clique em **mais** e, em seguida, clique na opção para visualizar todas as atualizações.	a. Clique em **Cluster > Overview**. b. Na seção **Visão geral**, clique em **mais** e, em seguida, clique em **Atualização do ONTAP**. c. Dependendo da sua versão do ONTAP, faça o seguinte: ◦ Para ONTAP 9.15,1 e anteriores, clique em **Atualização de firmware**. ◦ Para ONTAP 9.16,1 e posterior, clique em **todas as outras atualizações**. d. Na página de atualização, clique em **mais** e, em seguida, clique na opção para ver todas as atualizações.

2. Clique ao lado da descrição para exibir uma lista de ações que podem ser executadas na recomendação.

   Você pode executar uma das seguintes ações, dependendo do estado da recomendação:

Se a atualização estiver neste estado…	Você pode…
Não foi agendado	**Update**: Inicia o processo de atualização. **Agendamento**: Permite que você defina uma data para iniciar o processo de atualização. **Dismiss**: Remove a recomendação da lista.
Foi programado	**Update**: Inicia o processo de atualização. **Editar horário**: Permite modificar a data agendada para iniciar o processo de atualização. **Cancelar horário**: Cancela a data agendada.
Foi demitido	**Undismiss**: Retorna a recomendação para a lista.
Está a ser aplicado ou está a ser transferido	**Cancelar**: Cancela a atualização.

Atualize o firmware manualmente

A partir do ONTAP 9.9,1, se você estiver registrado no "Active IQ Unified Manager", poderá receber alertas no Gerenciador de sistema que o informam quando atualizações de firmware para dispositivos compatíveis, como disco, prateleiras de disco, processador de serviço (SP) ou controlador de gerenciamento de placa base (BMC) estiverem

pendentes no cluster.

Se você estiver executando o ONTAP 9.8 ou não estiver registrado no Active IQ Unified Manager, navegue até o site de suporte da NetApp para baixar as atualizações de firmware.

Antes de começar

Para se preparar para uma atualização de firmware suave, reinicie o SP ou o BMC antes de iniciar a atualização. Use o `system service-processor reboot-sp -node node_name` comando para reinicializar.

Passos

Siga o procedimento apropriado com base na sua versão do ONTAP e se estiver registado no Active IQ Unified Manager.

ONTAP 9.16,1 e posterior com Consultor Digital

Passos

1. No System Manager, vá para **Dashboard**.

   Na seção **Saúde**, uma mensagem será exibida se houver atualizações de firmware recomendadas para o cluster.

2. Clique na mensagem de alerta.
3. Ao lado das atualizações de segurança na lista de atualizações recomendadas, selecione **ações**.
4. Clique em **Atualizar** para instalar a atualização imediatamente ou **Agendar** para programá-la para mais tarde.

   Se a atualização já estiver agendada, você pode **Editar** ou **Cancelar**.

ONTAP 9.9,1 a 9.15.1 com Consultor Digital

1. No System Manager, vá para **Dashboard**.

   Na seção **Saúde**, uma mensagem será exibida se houver atualizações de firmware recomendadas para o cluster.

2. Clique na mensagem de alerta.

   A guia **Atualização de firmware** é exibida na página **Atualização**.

3. Clique em **Download do site de suporte da NetApp** para obter a atualização de firmware que você deseja executar.

   O site de suporte da NetApp é exibido.

4. Inicie sessão no site de suporte da NetApp e transfira o pacote de imagens de firmware necessário para a atualização.
5. Copie os arquivos para um servidor HTTP ou FTP em sua rede ou para uma pasta local.
6. No System Manager, clique em **Cluster > Overview**.
7. No canto direito do painel **Visão geral**, clique em **mais** ⋮ e selecione **Atualização do ONTAP**.
8. Clique em **Atualização de firmware**.
9. Dependendo da sua versão do ONTAP, faça o seguinte:

ONTAP 9.9,1 e 9.10.0	ONTAP 9.10,1 e posterior
a. Selecione **de servidor** ou **Cliente local** b. Forneça a URL do servidor ou a localização do arquivo.	a. Na lista de atualizações recomendadas, selecione **ações**. b. Clique em **Atualizar** para instalar a atualização imediatamente ou **Agendar** para programá-la para mais tarde. Se a atualização já estiver agendada, você pode **Editar** ou **Cancelar**. c. Selecione o botão **Atualizar firmware**.

ONTAP 9 F.8 e posterior sem Consultor Digital

1. Navegue até "Site de suporte da NetApp"e inicie sessão.
2. Selecione o pacote de firmware que pretende utilizar para atualizar o firmware do cluster.
3. Copie os arquivos para um servidor HTTP ou FTP em sua rede ou para uma pasta local.
4. No System Manager, clique em **Cluster > Overview**.
5. No canto direito do painel **Visão geral**, clique em **mais** ⋮ e selecione **Atualização ONTAP** ou **atualizações de software** (dependendo da sua versão).
6. Dependendo da sua versão do ONTAP, faça o seguinte:
   - Para ONTAP 9.15,1 e anteriores, clique em **Atualização de firmware**.
   - Para ONTAP 9.16,1 e posterior, clique em **todas as outras atualizações**.
7. Dependendo da sua versão do ONTAP, faça o seguinte:

ONTAP 9.8, 9,9.1, e 9.10.0	ONTAP 9.10,1 e posterior
1. Selecione **de servidor** ou **Cliente local** 2. Forneça a URL do servidor ou a localização do arquivo.	1. Na lista de atualizações recomendadas, selecione **ações**. 2. Clique em **Atualizar** para instalar a atualização imediatamente ou **Agendar** para programá-la para mais tarde. Se a atualização já estiver agendada, você pode **Editar** ou **Cancelar**. 3. Selecione o botão **Atualizar firmware**.

Depois de terminar

Você pode monitorar ou verificar atualizações em **Resumo da atualização de firmware**. Para exibir atualizações que foram descartadas ou não foram instaladas, siga um destes procedimentos, dependendo da sua versão do ONTAP:

- Para o ONTAP 9.15,1 e anteriores, clique em **Cluster > Definições > Atualização automática > Ver todas as atualizações automáticas**
- Para o ONTAP 9.16,1 e posterior, clique em **Cluster > Settings > Software updates**. No canto direito do

painel **todas as outras atualizações**, clique em **mais** ⋮ e selecione **Ver todas as atualizações automáticas**.

Reverter ONTAP

Preciso de suporte técnico para reverter um cluster do ONTAP?

Você deve entrar em Contato com o suporte técnico antes de tentar reverter um cluster do ONTAP nas seguintes situações:

- Um ambiente de produção

  Não tente reverter um cluster de produção sem a assistência do suporte técnico.

- Você criou volumes no ONTAP 9.5 ou posterior e precisa reverter para uma versão anterior.

  Os volumes que utilizam a compressão adaptável devem ser descomprimidos antes de reverter.

É possível reverter clusters novos ou de teste sem assistência. Se você tentar reverter um cluster sozinho e tiver algum dos seguintes problemas, ligue para o suporte técnico:

- A reversão falha ou não pode terminar.
- A reversão termina, mas o cluster não é utilizável em um ambiente de produção.
- A reversão termina e o cluster entra em produção, mas você não está satisfeito com seu comportamento.

Reverter caminhos de ONTAP compatíveis

Você pode reverter diretamente seu software ONTAP para apenas uma versão anterior à versão atual do ONTAP. Por exemplo, se você estiver executando 9.15.1, não poderá reverter diretamente para 9.13.1. Você deve reverter para 9.14.1; em seguida, executar uma reversão separada de 9.14.1 para 9.13.1.

Reverter para o ONTAP 9.4 ou anterior não é suportado. Você não deve reverter para versões sem suporte do ONTAP.

Você pode usar o `system image show` comando para determinar a versão do ONTAP em execução em cada nó.

Os seguintes caminhos de reversão compatíveis referem-se apenas a versões ONTAP locais. Para obter informações sobre como reverter o ONTAP na nuvem, "Revertendo ou baixando Cloud Volumes ONTAP" consulte .

Você pode reverter de…	Para…
ONTAP 9.16,1	ONTAP 9.15,1
ONTAP 9.15,1	ONTAP 9.14,1
ONTAP 9.14,1	ONTAP 9.13,1

Você pode reverter de…	Para…
ONTAP 9.13,1	ONTAP 9.12,1
ONTAP 9.12,1	ONTAP 9.11,1
ONTAP 9.11,1	ONTAP 9.10,1
ONTAP 9.10,1	ONTAP 9.9,1
ONTAP 9.9,1	ONTAP 9,8
ONTAP 9,8	ONTAP 9,7
ONTAP 9,7	ONTAP 9,6
ONTAP 9,6	ONTAP 9,5

ONTAP reverte problemas e limitações

Você precisa considerar os problemas de reversão e as limitações antes de reverter um cluster do ONTAP.

- Reversão é disruptiva.

  Nenhum acesso de cliente pode ocorrer durante a reversão. Se você estiver revertendo um cluster de produção, inclua essa interrupção no Planejamento.

- A reversão afeta todos os nós no cluster.

  A reversão afeta todos os nós no cluster; no entanto, a reversão deve ser realizada e concluída em cada par de HA antes que outros pares de HA sejam revertidos.

- A reversão é concluída quando todos os nós estão executando a nova liberação de destino.

  Quando o cluster está em um estado de versão mista, você não deve inserir nenhum comando que altere a operação ou configuração do cluster, exceto se necessário para atender aos requisitos de reversão; operações de monitoramento são permitidas.

  > Se você reverteu alguns, mas não todos os nós, não tente atualizar o cluster de volta para a versão de origem.

- Quando você reverte um nó, ele limpa os dados em cache em um módulo Flash Cache.

  Como não há dados armazenados em cache no módulo Flash Cache, o nó serve solicitações de leitura inicial do disco, o que resulta em menor desempenho de leitura durante esse período. O nó repreenche o cache à medida que serve solicitações de leitura.

- Um LUN que é feito backup em fita em execução no ONTAP 9.x pode ser restaurado apenas para 9.x e versões posteriores e não para uma versão anterior.

- Se sua versão atual do ONTAP oferecer suporte à funcionalidade ACP na banda (IBACP) e você reverter para uma versão do ONTAP que não suporte IBACP, o caminho alternativo para o compartimento de disco será desativado.
- Se o LDAP for usado por qualquer uma de suas máquinas virtuais de armazenamento (SVMs), a referência LDAP deve ser desativada antes da reversão.
- Em sistemas IP MetroCluster usando switches que são compatíveis com MetroCluster, mas não validados pela MetroCluster, a reversão do ONTAP 9.7 para o 9,6 é disruptiva, pois não há suporte para sistemas que usam o ONTAP 9.6 e anteriores.
- Antes de reverter um nó para o ONTAP 9.13,1 ou anterior, você precisa primeiro converter um volume raiz criptografado SVM para um volume não criptografado

  Se você tentar reverter para uma versão que não ofereça suporte à criptografia de volume raiz do SVM, o sistema responderá com um aviso e bloqueará a reversão.

Prepare-se para uma reversão do ONTAP

Recursos a serem analisados antes de reverter um cluster do ONTAP

Antes de reverter um cluster do ONTAP, você deve confirmar o suporte a hardware e analisar os recursos para entender os problemas que você pode encontrar ou precisar resolver.

1. Reveja "ONTAP 9 Notas de versão"a para obter a versão alvo.

   A seção ""atenção importante"" descreve possíveis problemas que você deve estar ciente antes de baixar ou reverter.

2. Confirme se sua plataforma de hardware é suportada na versão de destino.

   "NetApp Hardware Universe"

3. Confirme se o cluster e os switches de gerenciamento são suportados na versão de destino.

   Você deve verificar se as versões de software NX-os (switches de rede de cluster), IOS (switches de rede de gerenciamento) e arquivo de configuração de referência (RCF) são compatíveis com a versão do ONTAP para a qual você está revertendo.

   "Downloads do NetApp: Comutador Ethernet Cisco"

4. Se o cluster estiver configurado para SAN, confirme se a configuração SAN é totalmente suportada.

   Todos os componentes SAN, incluindo a versão do software ONTAP de destino, o sistema operacional do host e patches, o software de utilitários de host necessários e os drivers e firmware do adaptador, devem ser suportados.

   "Ferramenta de Matriz de interoperabilidade do NetApp"

Verificações do sistema a serem executadas antes de reverter um cluster ONTAP

Antes de reverter um cluster do ONTAP, verifique a integridade do cluster, a integridade do storage e a hora do sistema. Você também deve verificar se nenhum trabalho está

sendo executado no cluster.

Verifique a integridade do cluster

Antes de reverter um cluster do ONTAP, verifique se os nós estão íntegros e qualificados para participar do cluster e se o cluster está quórum.

Passos

1. Verifique se os nós do cluster estão online e estão qualificados para participar do cluster:

   ```
   cluster show
   ```

   Neste exemplo, todos os nós estão íntegros e qualificados para participar do cluster.

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   Se algum nó não for saudável ou não for elegível, verifique se há erros nos logs do EMS e tome medidas corretivas.

2. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

   Entre `y` para continuar.

3. Verifique os detalhes de configuração para cada processo RDB.

   - A época do banco de dados relacional e as epochs do banco de dados devem corresponder para cada nó.
   - O mestre de quórum por anel deve ser o mesmo para todos os nós.

     Observe que cada anel pode ter um mestre de quórum diferente.

Para exibir este processo RDB…	Digite este comando…
Aplicação de gerenciamento	`cluster ring show -unitname mgmt`
Base de dados de localização de volume	`cluster ring show -unitname vldb`

Para exibir este processo RDB…	Digite este comando…
Gerenciador de interface virtual	`cluster ring show -unitname vifmgr`
Daemon de gerenciamento SAN	`cluster ring show -unitname bcomd`

Este exemplo mostra o processo do banco de dados de localização de volume:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

5. Se você estiver operando em um ambiente SAN, verifique se cada nó está em um quórum de SAN:

```
event log show  -severity informational -message-name scsiblade.*
```

A mensagem de evento scsipblade mais recente para cada nó deve indicar que o scsi-blade está em quórum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Informações relacionadas

"Administração do sistema"

Verifique a integridade do armazenamento

Antes de reverter um cluster do ONTAP, verifique o status dos discos, agregados e volumes.

Passos

1. Verifique o status do disco:

Para verificar…	Faça isso…
Discos quebrados	a. Exibir todos os discos quebrados: `storage disk show -state broken` b. Remova ou substitua quaisquer discos quebrados.
Discos em manutenção ou reconstrução	a. Exiba todos os discos em estados de manutenção, pendentes ou reconstrução: `storage disk show -state maintenance`
pending	reconstructing ---- .. Aguarde até que a operação de manutenção ou reconstrução termine antes de prosseguir.

2. Verifique se todos os agregados estão online, exibindo o estado do storage físico e lógico, incluindo agregados de storage

```
storage aggregate show -state !online
```

Este comando exibe os agregados que estão *não* online. Todos os agregados devem estar online antes e depois de realizar uma grande atualização ou reversão.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verifique se todos os volumes estão online exibindo quaisquer volumes que estejam *não* online:

```
volume show -state !online
```

Todos os volumes devem estar online antes e depois de realizar uma grande atualização ou reversão.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verifique se não existem volumes inconsistentes:

```
volume show -is-inconsistent true
```

Consulte o artigo da base de dados de Conhecimento "Volume Mostrando WAFL inconsistente"sobre como resolver os volumes inconsistentes.

Informações relacionadas

"Gerenciamento de disco e agregado"

Verifique a hora do sistema

Antes de reverter um cluster ONTAP, você deve verificar se o NTP está configurado e se o tempo está sincronizado no cluster.

Passos

1. Verifique se o cluster está associado a um servidor NTP:

```
cluster time-service ntp server show
```

2. Verifique se cada nó tem a mesma data e hora:

```
cluster date show
```

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

Verifique se nenhum trabalho está em execução

Antes de reverter um cluster do ONTAP, verifique o status dos trabalhos do cluster. Se qualquer agregado, volume, NDMP (despejo ou restauração) ou trabalhos Snapshot (como criar, excluir, mover, modificar, replicar e montar trabalhos) estiver em execução ou na fila, você deverá permitir que os trabalhos terminem com êxito ou interrompam as entradas na fila.

Passos

1. Revise a lista de tarefas de agregado, volume ou Snapshot em execução ou na fila:

   ```
   job show
   ```

   Neste exemplo, existem dois trabalhos em fila:

   ```
   cluster1::> job show
                              Owning
   Job ID Name                Vserver    Node           State
   ------ ------------------- ---------- -------------- ----------
   8629   Vol Reaper          cluster1   -              Queued
          Description: Vol Reaper Job
   8630   Certificate Expiry Check
                              cluster1   -              Queued
          Description: Certificate Expiry Check
   ```

2. Exclua quaisquer trabalhos de cópia de agregado, volume ou Snapshot em execução ou na fila:

   ```
   job delete -id <job_id>
   ```

3. Verifique se nenhum agregado, volume ou trabalhos Snapshot estão em execução ou na fila:

   ```
   job show
   ```

   Neste exemplo, todos os trabalhos em execução e em fila foram excluídos:

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

Execute verificações de pré-reversão específicas da versão do ONTAP

Pré-reverter tarefas necessárias para a sua versão do ONTAP

Dependendo da versão do ONTAP, talvez seja necessário executar tarefas preparatórias adicionais antes de iniciar o processo de reversão.

Se você está revertendo de …	Faça o seguinte antes de iniciar o processo de reversão…
Qualquer versão do ONTAP 9	• "Encerrar sessões SMB que não estão continuamente disponíveis". • "Reveja os requisitos de reversão para relacionamentos SnapMirror e SnapVault". • "Verifique se os volumes desduplicados têm espaço livre suficiente". • "Preparar instantâneos". • "Defina o período de confirmação automática para volumes SnapLock como horas". • Se tiver uma configuração do MetroCluster, "desativar switchover não planejado automático".
ONTAP 9.16,1	• Se você tiver o TLS configurado para conexões NVMe/TCP, "Desative a configuração TLS nos hosts NVMe". • Se o monitoramento de desempenho de qtree estendido estiver ativado, "desative-o.". • Se você estiver usando CORS para acessar seus buckets do ONTAP S3, "Extrair a configuração CORS".
ONTAP 9.14,1	Se você tiver ativado o entroncamento para conexões de cliente, "Desative o entroncamento em qualquer servidor NFSv4,1".

Se você está revertendo de …	Faça o seguinte antes de iniciar o processo de reversão…
ONTAP 9.12,1	• Se você configurou o acesso de cliente S3 para dados nas, "Retire a configuração do balde nas S3." • Se você estiver executando o protocolo NVMe e tiver configurado a autenticação na banda, "desativar a autenticação na banda". • Se tiver uma configuração do MetroCluster, "Desativar IPsec".
ONTAP 9.11,1	Se você configurou o Autonomous ransomware Protection (ARP), "Verifique o licenciamento ARP".
ONTAP 9,6	Se você tiver relações síncronas do SnapMirror"prepare os relacionamentos para reverter", .

Qualquer versão do ONTAP 9

Encerre determinadas sessões SMB antes de reverter o ONTAP

Antes de reverter um cluster do ONTAP a partir de qualquer versão do ONTAP 9, você deve identificar e encerrar graciosamente todas as sessões de SMB que não estejam disponíveis continuamente.

Compartilhamentos SMB continuamente disponíveis, que são acessados por clientes Hyper-V ou Microsoft SQL Server usando o protocolo SMB 3,0, não precisam ser encerrados antes de atualizar ou fazer downgrade.

Passos

1. Identifique quaisquer sessões SMB estabelecidas que não estejam disponíveis continuamente:

   ```
   vserver cifs session show -continuously-available No -instance
   ```

   Este comando exibe informações detalhadas sobre quaisquer sessões SMB que não tenham disponibilidade contínua. Você deve encerrá-los antes de prosseguir com o downgrade do ONTAP.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
           Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. Se necessário, identifique os arquivos que estão abertos para cada sessão SMB que você identificou:

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

Requisitos de reversão do ONTAP para relacionamentos SnapMirror e SnapVault

O `system node revert-to` comando notifica você sobre quaisquer relações SnapMirror e SnapVault que precisam ser excluídas ou reconfiguradas para que o processo de reversão seja concluído. No entanto, você deve estar ciente desses requisitos antes de iniciar a reversão.

- Todos os relacionamentos de espelhamento de proteção de dados e SnapVault precisam estar quietos e quebrados.

  Depois que a reversão for concluída, você poderá ressincronizar e retomar esses relacionamentos se houver uma cópia Snapshot comum.

- Os relacionamentos do SnapVault não devem conter os seguintes tipos de diretiva do SnapMirror:
  - espelho assíncrono

    Você deve excluir qualquer relacionamento que use esse tipo de política.

  - MirrorAndVault

    Se algum desses relacionamentos existir, você deve alterar a política do SnapMirror para mirror-Vault.

- Todas as relações de espelhamento de compartilhamento de carga e volumes de destino devem ser excluídos.
- As relações do SnapMirror com volumes de destino do FlexClone devem ser excluídas.
- A compactação de rede deve ser desativada para cada política do SnapMirror.
- A regra all_source_snapshot deve ser removida de qualquer tipo de diretiva SnapMirror assíncrona-mirror.

  As operações Single File Snapshot Restore (SFSR) e Partial File Snapshot Restore (PFSR) são obsoletas no volume raiz.

- Todas as operações de restauração do Snapshot em execução no momento devem ser concluídas antes que a reversão possa continuar.

  Você pode esperar que a operação de restauração seja concluída ou pode abortá-la.

- Todas as operações de restauração do Snapshot e arquivo único incompleto devem ser removidas usando o `snapmirror restore` comando.

Verifique o espaço livre para volumes desduplicados antes de reverter o ONTAP

Antes de reverter um cluster do ONTAP a partir de qualquer versão do ONTAP 9, é necessário garantir que os volumes contenham espaço livre suficiente para a operação de reversão.

O volume deve ter espaço suficiente para acomodar as economias que foram obtidas através da deteção em linha de blocos de zeros. Consulte o artigo da base de dados de Conhecimento "Como ver economia de espaço com deduplicação, compressão e compactação no ONTAP 9".

Se você ativou a deduplicação e a compactação de dados em um volume que deseja reverter, então você deve reverter a compactação de dados antes de reverter a deduplicação.

Passos

1. Veja o progresso das operações de eficiência que estão sendo executadas nos volumes:

```
volume efficiency show -fields vserver,volume,progress
```

2. Parar todas as operações de deduplicação ativas e enfileiradas:

```
volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
```

3. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

4. Faça o downgrade dos metadados de eficiência de um volume para a versão de destino do ONTAP:

```
volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
-version <version>
```

O exemplo a seguir reverte os metadados de eficiência no volume VolA para ONTAP 9.x.

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```

> O comando revert-to de eficiência de volume reverte volumes que estão presentes no nó em que este comando é executado. Este comando não reverte volumes entre nós.

5. Monitorize o progresso do downgrade:

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. Se a reversão não for bem-sucedida, exiba a instância para ver por que a reversão falhou.

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. Depois que a operação Reverter estiver concluída, retorne ao nível de privilégio admin:

```
set -privilege admin
```

Saiba mais "Gerenciamento de storage lógico"sobre o .

Prepare instantâneos antes de reverter um cluster ONTAP

Antes de reverter um cluster do ONTAP de qualquer versão do ONTAP 9, desative todas as políticas de cópia Snapshot e exclua todas as cópias Snapshot criadas após a atualização para a versão atual.

Se você estiver revertendo em um ambiente SnapMirror, primeiro você deve excluir as seguintes relações de espelhamento:

- Todas as relações de espelhamento de compartilhamento de carga
- Todas as relações espelhadas de proteção de dados que foram criadas no ONTAP 8,3.x
- Todas as relações espelhadas de proteção de dados se o cluster foi recriado no ONTAP 8,3.x

Passos

1. Desative as políticas de cópia Snapshot para todos os SVMs de dados:

```
volume snapshot policy modify -vserver * -enabled false
```

2. Desative as políticas de cópia Snapshot para os agregados de cada nó:
   a. Identificar os agregados do nó:

```
run -node <nodename> -command aggr status
```

   b. Desative a política de cópia Snapshot para cada agregado:

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

   c. Repita esta etapa para cada nó restante.
3. Desative as políticas de cópia Snapshot para o volume raiz de cada nó:
   a. Identificar o volume raiz do nó:

```
run-node <node_name> -command vol status
```

   Você identifica o volume raiz pela palavra root na coluna **Opções** da `vol status` saída do comando.

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

a. Desative a política de cópia Snapshot no volume raiz:

```
run -node <node_name> vol options root_volume_name nosnap on
```

b. Repita esta etapa para cada nó restante.

4. Exclua todas as cópias Snapshot criadas após a atualização para a versão atual:

a. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

b. Desativar os instantâneos:

```
snapshot policy modify -vserver * -enabled false
```

c. Exclua as cópias Snapshot da versão mais recente do nó:

```
volume snapshot prepare-for-revert -node <node_name>
```

Esse comando exclui as cópias Snapshot da versão mais recente em cada volume de dados, agregado de raiz e volume raiz.

Se nenhuma cópia Snapshot não puder ser excluída, o comando falhará e notificará você de todas as ações necessárias que você deve tomar antes que as cópias snapshot possam ser excluídas. Você deve concluir as ações necessárias e executar novamente o `volume snapshot prepare-for-revert` comando antes de prosseguir para a próxima etapa.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all Snapshot copies that have the
format used by the current version of ONTAP. It will fail if any
Snapshot copy polices are enabled, or
         if any Snapshot copies have an owner. Continue? {y|n}: y
```

a. Verifique se as cópias Snapshot foram excluídas:

```
volume snapshot show -node nodename
```

b. Se houver cópias Snapshot da versão mais recente, force-as a serem excluídas:

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
-constituent true} -ignore-owners -force
```

c. Repita estas etapas para cada nó restante.

d. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Siga estas etapas nos dois clusters na configuração do MetroCluster.

Defina períodos de confirmação automática para volumes SnapLock antes de reverter o ONTAP

Antes de reverter um cluster do ONTAP a partir de qualquer versão do ONTAP 9, o valor do período de confirmação automática para volumes do SnapLock deve ser definido em horas, não em dias. Você deve verificar o valor de confirmação automática dos volumes do SnapLock e modificá-lo de dias para horas, se necessário.

Passos

1. Verifique se existem volumes SnapLock no cluster que têm períodos de confirmação automática não suportados:

```
volume snaplock show -autocommit-period *days
```

2. Modifique os períodos de confirmação automática não suportados para horas

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

Desative o switchover não planejado automático antes de reverter configurações de MetroCluster de dois nós e quatro nós

Antes de reverter uma configuração MetroCluster de dois nós ou quatro nós executando qualquer versão do ONTAP 9, você deve desativar o switchover não planejado automático (AUSO).

Passo

1. Em ambos os clusters no MetroCluster, desative o switchover não planejado automático:

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

Informações relacionadas

"Gerenciamento de MetroCluster e recuperação de desastres"

ONTAP 9.16,1

Desative o TLS em hosts NVMe antes de reverter do ONTAP 9.16.1

Se você tiver um canal seguro TLS para conexões NVMe/TCP configurado em um host NVMe, será necessário desativá-lo antes de reverter o cluster do ONTAP 9.16.1.

Passos

1. Remova a configuração de canal seguro TLS do host:

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

   Este comando remove o host do subsistema e, em seguida, recria o host no subsistema sem a configuração TLS.

2. Verifique se o canal seguro TLS é removido do host:

```
vserver nvme subsystem host show
```

Desative o monitoramento de desempenho estendido do Qtree antes de reverter do ONTAP 9.16.1

A partir do ONTAP 9.16,1, você pode usar a API REST do ONTAP para acessar os recursos estendidos de monitoramento de qtree, que incluem métricas de latência e estatísticas históricas. Se o monitoramento de qtree estendido estiver ativado em qualquer qtrees, antes de reverter do 9.16.1, você deve definir `ext_performance_monitoring.enabled` como false.

Saiba mais "reverter clusters com monitoramento de desempenho de qtree estendido"sobre o .

Remova a configuração CORS antes de reverter do ONTAP 9.16.1

Se você estiver usando o Compartilhamento de recursos entre origens (CORS) para acessar os buckets do ONTAP S3, será necessário removê-lo antes de reverter do ONTAP 9.16.1.

Saiba mais "Revertendo clusters ONTAP com o uso de CORS"sobre o .

ONTAP 9.14,1

Desative o entroncamento de sessão NFSv4,1 antes de reverter do ONTAP 9.14.1

Se você ativou o entroncamento para conexões de cliente, você deve desativar o entroncamento em qualquer servidor NFSv4,1 antes de reverter do ONTAP 9.14.1.

Ao inserir o `revert-to` comando, você verá uma mensagem de aviso aconselhando você a desativar o entroncamento antes de prosseguir.

Depois de reverter para um ONTAP 9.13.1, os clientes que usam conexões truncadas voltam para usar uma única conexão. A taxa de transferência de dados será afetada, mas não haverá interrupções. O comportamento de reversão é o mesmo que modificar a opção de entroncamento NFSv4,1 para o SVM de habilitado para desativado.

Passos

1. Desative o entroncamento no servidor NFSv4,1:

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. Verifique se o NFS está configurado conforme desejado:

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12,1

Remova a configuração do bucket nas S3 antes de reverter do ONTAP 9.12.1

Se você configurou o acesso de cliente S3 para dados nas, você deve usar a interface de linha de comando (CLI) do ONTAP para remover a configuração do bucket do nas e remover quaisquer mapeamentos de nomes (usuários S3 para usuários Windows ou Unix) antes de reverter do ONTAP 9.12.1.

Sobre esta tarefa

As tarefas a seguir são concluídas em segundo plano durante o processo de reversão.

- Remova todas as criações de objetos singleton parcialmente concluídas (isto é, todas as entradas em diretórios ocultos).
- Remova todos os diretórios ocultos; pode haver um em para cada volume acessível a partir da raiz da exportação mapeada a partir do bucket do nas S3.
- Remova a tabela de carregamento.
- Exclua todos os valores padrão-unix-user e padrão-Windows-user para todos os servidores S3 configurados.

Passos

1. Remova a configuração do balde nas S3:

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket
<s3_nas_bucket_name>
```

2. Remover mapeamentos de nomes para UNIX:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

3. Remover mapeamentos de nomes para Windows:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. Remova os protocolos S3 da SVM:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Desative a autenticação NVMe na banda antes de reverter a partir do ONTAP 9.12.1

Se você estiver executando o protocolo NVMe, desative a autenticação na banda antes de reverter o cluster do ONTAP 9.12.1. Se a autenticação na banda usando DH-HMAC-CHAP não estiver desativada, a reversão falhará.

Passos

1. Remova o host do subsistema para desativar a autenticação DH-HMAC-CHAP:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verifique se o protocolo de autenticação DH-HMAC-CHAP foi removido do host:

```
vserver nvme subsystem host show
```

3. Adicione o host de volta ao subsistema sem autenticação:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Desative o IPsec nas configurações do MetroCluster antes de reverter a partir do ONTAP 9.12.1

Antes de reverter uma configuração do MetroCluster do ONTAP 9.12.1, você deve desativar o IPsec.

Uma verificação é realizada antes da reversão para garantir que não haja configurações IPsec na configuração do MetroCluster. Você deve remover todas as configurações IPsec presentes e desativar o IPsec antes de continuar com a reversão. A reversão do ONTAP será bloqueada se o IPsec estiver habilitado, mesmo quando você não tiver configurado nenhuma diretiva de usuário.

ONTAP 9.11,1

Verifique o licenciamento do Autonomous ransomware Protection antes de reverter do ONTAP 9.11.1

Se você configurou o ARP (Autonomous ransomware Protection) e reverte do ONTAP 9.11.1 para o ONTAP 9.10.1, você pode ter mensagens de aviso e funcionalidade ARP limitada.

No ONTAP 9.11,1, a licença Anti-ransomware substituiu a licença de Gerenciamento de chaves de vários locatários (MTKM). Se o seu sistema tiver a licença Anti_ransomware, mas nenhuma licença MT_EK_MGMT, você verá um aviso durante a reversão de que o ARP não pode ser ativado em novos volumes após a reversão.

Os volumes com proteção existente continuarão a funcionar normalmente após a reversão e o status ARP pode ser exibido usando a CLI do ONTAP. O System Manager não pode mostrar o status ARP sem a licença MTKM.

Portanto, se você quiser que o ARP continue depois de reverter para o ONTAP 9.10,1, certifique-se de que a licença MTKM esteja instalada antes de reverter. "Saiba mais sobre o licenciamento ARP."

ONTAP 9,6

Considerações para reverter sistemas de ONTAP 9,6 com relações síncronas SnapMirror

Você deve estar ciente das considerações para relacionamentos síncronos do SnapMirror antes de reverter do ONTAP 9.6 para o ONTAP 9.5.

Antes de reverter, você deve seguir as seguintes etapas se tiver relações síncronas do SnapMirror:

- É necessário excluir qualquer relacionamento síncrono do SnapMirror no qual o volume de origem esteja fornecendo dados usando NFSv4 ou SMB.

  O ONTAP 9.5 não oferece suporte a NFSv4 e SMB.

- Você deve excluir quaisquer relações síncronas do SnapMirror em uma implantação em cascata espelhada.

  Uma implantação em cascata espelhada não é suportada para relacionamentos síncronos do SnapMirror no ONTAP 9.5.

- Se as cópias Snapshot comuns no ONTAP 9.5 não estiverem disponíveis durante a reversão, será necessário inicializar o relacionamento síncrono do SnapMirror após a reversão.

  Após duas horas de atualização para o ONTAP 9.6, as cópias Snapshot comuns do ONTAP 9.5 são automaticamente substituídas pelas cópias Snapshot comuns no ONTAP 9.6. Portanto, não é possível ressincronizar a relação síncrona do SnapMirror após reverter se as cópias Snapshot comuns do ONTAP 9.5 não estiverem disponíveis.

Transfira e instale a imagem do software ONTAP

Antes de reverter o software ONTAP atual, você deve baixar a versão de software de destino no site de suporte da NetApp e instalá-la.

Transfira a imagem do software ONTAP

As imagens de software são específicas para modelos de plataforma. Tem de obter a imagem correta para o cluster. Imagens de software, informações sobre a versão do firmware e o firmware mais recente para o modelo da sua plataforma estão disponíveis no site de suporte da NetApp. As imagens de software incluem a versão mais recente do firmware do sistema que estava disponível quando uma determinada versão do ONTAP foi lançada.

> Se estiver a reverter um sistema com encriptação de volume NetApp a partir do ONTAP 9,5 ou posterior, tem de transferir a imagem do software ONTAP para países não restritos, que inclui encriptação de volume NetApp. Se você usar a imagem do software ONTAP para países restritos para reverter um sistema com criptografia de volume NetApp, o sistema fica em pânico e você perde o acesso aos volumes.

Passos

1. Localize o software ONTAP de destino na "Transferências de software" área do site de suporte da NetApp.
2. Copie a imagem do software (por exemplo, 97_q_image.tgz) do site de suporte da NetApp

   Você pode copiar a imagem para o diretório no servidor HTTP ou servidor FTP do qual a imagem será servida ou para uma pasta local.

Instale a imagem do software ONTAP

Depois de fazer o download da imagem do software ONTAP de destino a partir do site de suporte do NetApp, instale-a nos nós do cluster.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

   (`*>`É apresentado o aviso avançado).

2. Digite `y` para continuar quando solicitado .
3. Instale a imagem do software:
   - Para configurações padrão ou uma configuração de MetroCluster de dois nós, digite o seguinte comando:

     ```
     system node image update -node * -package location -replace-package
     true -setdefault true -background true
     ```

     Este comando faz o download e instala a imagem do software em todos os nós simultaneamente. Para baixar e instalar a imagem em cada nó, uma de cada vez, não especifique o `-background` parâmetro. Este comando também usa uma consulta estendida para alterar a imagem do software de destino, que é instalada como imagem alternativa, para ser a imagem padrão para o nó.

   - Para uma configuração de MetroCluster de quatro ou oito nós, digite o seguinte comando em ambos os clusters:

```
system node image update -node * -package location -replace-package
true true -background true -setdefault false
```

Este comando faz o download e instala a imagem do software em todos os nós simultaneamente. Para baixar e instalar a imagem em cada nó, uma de cada vez, não especifique o `-background` parâmetro. Este comando também usa uma consulta estendida para alterar a imagem do software de destino, que é instalada como a imagem alternativa em cada nó.

4. Digite `y` para continuar quando solicitado.
5. Verifique se a imagem do software foi baixada e instalada em cada nó:

```
system node image show-update-progress -node *
```

Este comando exibe o status atual do download e instalação da imagem do software. Você deve continuar a executar este comando até que todos os nós relatem um **Status de execução** de "sair" e um **Status de saída** de "sucesso".

O comando de atualização da imagem do nó do sistema pode falhar e apresentar mensagens de erro ou aviso. Depois de resolver quaisquer erros ou avisos, você pode executar o comando novamente.

Este exemplo mostra um cluster de dois nós no qual a imagem do software é baixada e instalada com sucesso em ambos os nós:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Reverter um cluster ONTAP

Reverter um cluster ONTAP causa interrupções. Você deve colocar o cluster off-line durante a reversão. Você não deve reverter um cluster de produção sem a assistência do

suporte técnico.

Para reverter um cluster novo ou de teste, você deve desativar failover de armazenamento e LIFs de dados e pré-condições de reversão de endereço; em seguida, você deve reverter a configuração do cluster e do sistema de arquivos em cada nó no cluster.

Antes de começar.

- Você deve ter concluído o "verificações pré-revertidas".
- Você deve ter concluído o "Pré-verificações para sua versão específica do ONTAP"necessário .

Passo 1: Prepare o cluster para reversão

Antes de reverter qualquer um dos nós de cluster, você deve verificar se a imagem do ONTAP de destino está instalada e desativar todas as LIFs de dados no cluster.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

   Digite **y** quando solicitado a continuar.

2. Verifique se o software ONTAP de destino está instalado:

   ```
   system image show
   ```

   O exemplo a seguir mostra que a versão 9.13.1 está instalada como a imagem alternativa em ambos os nós:

   ```
   cluster1::*> system image show
                    Is      Is                    Install
   Node     Image   Default Current Version    Date
   -------- ------- ------- ------- --------   -------------------
   node0
            image1  true    true    9.14.1      MM/DD/YYYY TIME
            image2  false   false   9.13.1      MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1      MM/DD/YYYY TIME
            image2  false   false   9.13.1      MM/DD/YYYY TIME
   4 entries were displayed.
   ```

3. Desative todas as LIFs de dados no cluster:

   ```
   network interface modify {-role data} -status-admin down
   ```

4. Determine se você tem relacionamentos FlexCache entre clusters:

```
flexcache origin show-caches -relationship-type inter-cluster
```

5. Se os flexcaches entre clusters estiverem presentes, desative os dados de vida no cluster de cache:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -status
-admin down
```

Etapa 2: Reverter nós de cluster

Para reverter o cluster, você precisa reverter o primeiro nó em um par de HA e, em seguida, reverter o nó de parceiro. Em seguida, repita esse processo para cada par de HA no cluster até que todos os nós sejam revertidos. Se você tiver uma configuração do MetroCluster, precisará repetir essas etapas para ambos os clusters na configuração.

4 ou mais nós

Passos

1. Faça login no nó que você deseja reverter.

   Para reverter um nó, você deve estar conetado ao cluster por meio do LIF de gerenciamento de nós do nó.

2. Desative o failover de storage para os nós no par de HA:

   ```
   storage failover modify -node <nodename> -enabled false
   ```

   Você só precisa desativar o failover de storage uma vez para o par de HA. Quando você desativa o failover de armazenamento para um nó, o failover de armazenamento também é desativado no parceiro do nó.

3. Defina a imagem de software ONTAP de destino do nó para ser a imagem padrão:

   ```
   system image modify -node <nodename> -image <target_image>
   -isdefault true
   ```

4. Verifique se a imagem do software ONTAP de destino está definida como a imagem padrão para o nó que você está revertendo:

   ```
   system image show
   ```

   O exemplo a seguir mostra que a versão 9.13.1 está definida como a imagem padrão no node0:

   ```
   cluster1::*> system image show
                    Is      Is                  Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- --------    -------------------
   node0
            image1  false   true    9.14.1       MM/DD/YYYY TIME
            image2  true    false   9.13.1       MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1       MM/DD/YYYY TIME
            image2  false   false   9.13.1       MM/DD/YYYY TIME
   4 entries were displayed.
   ```

5. Verifique se o nó está pronto para reversão:

   ```
   system node revert-to -node <nodename> -check-only true -version 9.x
   ```

O `check-only` parâmetro identifica quaisquer pré-condições que devem ser abordadas antes de reverter, como desabilitar a política Snapshot ou excluir cópias Snapshot que foram criadas após a atualização para a versão posterior do ONTAP.

6. Reverter a configuração do cluster do nó:

```
system node revert-to -node <nodename> -version 9.x
```

A `-version` opção refere-se à versão ONTAP para a qual você está revertendo. Por exemplo, se você estiver revertendo de 9.14.1 para 9.13.1, o valor correto `-version` da opção é 9.13.1.

A configuração do cluster é revertida e, em seguida, você é desconetado do clustershell.

7. Aguarde o prompt de login; em seguida, digite **não** quando você for perguntado se deseja fazer login no systemshell.

Pode demorar até 30 minutos ou mais para que o prompt de login apareça.

8. Faça login no clustershell com admin.
9. Mude para o nodeshell:

```
run -node <nodename>
```

Depois de fazer login no clustershell novamente, pode demorar alguns minutos até que ele esteja pronto para aceitar o comando nodeshell. Então, se o comando falhar, aguarde alguns minutos e tente novamente.

10. Reverter a configuração do sistema de arquivos do nó:

```
revert_to 9.x
```

Este comando verifica se a configuração do sistema de arquivos do nó está pronta para ser revertida e, em seguida, reverte-a. Se quaisquer pré-condições forem identificadas, você deve abordá-las e, em seguida, executar novamente o `revert_to` comando.

Usar um console do sistema para monitorar o processo de reversão exibe maiores detalhes do que o visto no nodeshell.

Se AUTOBOOT for true, quando o comando terminar, o nó será reiniciado para ONTAP.

Se AUTOBOOT for false, quando o comando terminar, o prompt Loader será exibido. Digite `yes` para reverter; em seguida, use `boot_ontap` para reinicializar manualmente o nó.

11. Depois que o nó reiniciar, confirme se o novo software está em execução:

```
system node image show
```

No exemplo a seguir, image1 é a nova versão do ONTAP e é definida como a versão atual no node0:

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image   Default Current Version     Date
-------- ------- ------- ------- --------    -------------------
node0
         image1  true    true    X.X.X        MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X       MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

12. Verifique se o status de reversão para o nó está concluído:

```
system node upgrade-revert show -node <nodename>
```

O status deve ser listado como "completo", "não necessário" ou "não há entradas de tabela retornadas."

13. Repita essas etapas no outro nó do par de HA e, em seguida, repita essas etapas para cada par de HA adicional.

Se você tiver uma Configuração do MetroCluster, precisará repetir essas etapas em ambos os clusters na configuração

14. Depois de todos os nós terem sido revertidos, reative a alta disponibilidade para o cluster:

```
cluster ha modify -configured true
```

cluster de 2 nós

1. Faça login no nó que você deseja reverter.

Para reverter um nó, você deve estar conetado ao cluster por meio do LIF de gerenciamento de nós do nó.

2. Desativar a alta disponibilidade do cluster (HA):

```
cluster ha modify -configured false
```

3. Desativar failover de armazenamento:

```
storage failover modify -node <nodename> -enabled false
```

Você só precisa desativar o failover de storage uma vez para o par de HA. Quando você desativa o failover de armazenamento para um nó, o failover de armazenamento também é desativado no parceiro do nó.

4. Defina a imagem de software ONTAP de destino do nó para ser a imagem padrão:

```
system image modify -node <nodename> -image <target_image>
-isdefault true
```

5. Verifique se a imagem do software ONTAP de destino está definida como a imagem padrão para o nó que você está revertendo:

```
system image show
```

O exemplo a seguir mostra que a versão 9,1 está definida como a imagem padrão no node0:

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   false   true    9.2         MM/DD/YYYY TIME
         image2   true    false   9.1         MM/DD/YYYY TIME
node1
         image1   true    true    9.2         MM/DD/YYYY TIME
         image2   false   false   9.1         MM/DD/YYYY TIME
4 entries were displayed.
```

6. Verifique se o nó atualmente contém epsilon:

```
cluster show -node <nodename>
```

O exemplo a seguir mostra que o nó contém epsilon:

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

a. Se o nó possuir epsilon, marque epsilon como false no nó para que o epsilon possa ser transferido para o parceiro do nó:

```
cluster modify -node <nodename> -epsilon false
```

b. Transfira o epsilon para o parceiro do nó marcando o epsilon true no nó do parceiro:

```
cluster modify -node <node_partner_name> -epsilon true
```

7. Verifique se o nó está pronto para reversão:

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

O `check-only` parâmetro identifica quaisquer condições que devem ser abordadas antes de reverter, como desabilitar a política de snapshot ou excluir cópias snapshot que foram criadas após a atualização para a versão posterior do ONTAP.

8. Reverter a configuração do cluster do nó:

```
system node revert-to -node <nodename> -version 9.x
```

A `-version` opção refere-se à versão ONTAP para a qual você está revertendo. Por exemplo, se você estiver revertendo de 9.14.1 para 9.13.1, o valor correto `-version` da opção é 9.13.1.

A configuração do cluster é revertida e, em seguida, você é desconetado do clustershell.

9. Aguarde o prompt de login; em seguida, digite `No` quando você for perguntado se deseja fazer login no systemshell.

Pode demorar até 30 minutos ou mais para que o prompt de login apareça.

10. Faça login no clustershell com admin.
11. Mude para o nodeshell:

```
run -node <nodename>
```

Depois de fazer login no clustershell novamente, pode demorar alguns minutos até que ele esteja pronto para aceitar o comando nodeshell. Então, se o comando falhar, aguarde alguns minutos e tente novamente.

12. Reverter a configuração do sistema de arquivos do nó:

```
revert_to 9.x
```

Este comando verifica se a configuração do sistema de arquivos do nó está pronta para ser revertida e, em seguida, reverte-a. Se quaisquer pré-condições forem identificadas, você deve abordá-las e, em seguida, executar novamente o `revert_to` comando.

> Usar um console do sistema para monitorar o processo de reversão exibe maiores detalhes do que o visto no nodeshell.

Se AUTOBOOT for true, quando o comando terminar, o nó será reiniciado para ONTAP.

Se AUTOBOOT for false, quando o comando terminar, o prompt Loader será exibido. Digite `yes` para reverter; em seguida, use `boot_ontap` para reinicializar manualmente o nó.

13. Depois que o nó reiniciar, confirme se o novo software está em execução:

```
system node image show
```

No exemplo a seguir, image1 é a nova versão do ONTAP e é definida como a versão atual no node0:

```
cluster1::*> system node image show
                Is      Is                  Install
Node     Image  Default Current Version     Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  true    true    X.X.X       MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X      MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

14. Verifique se o status Reverter está concluído para o nó:

```
system node upgrade-revert show -node <nodename>
```

O status deve ser listado como "completo", "não necessário" ou "não há entradas de tabela retornadas."

15. Repita essas etapas no outro nó no par de HA.
16. Depois que ambos os nós tiverem sido revertidos, reative a alta disponibilidade para o cluster:

```
cluster ha modify -configured true
```

17. Reative o failover de storage em ambos os nós:

```
storage failover modify -node <nodename> -enabled true
```

O que fazer depois de um ONTAP Reverter

Verifique a integridade do cluster e do storage após uma reversão do ONTAP

Depois de reverter um cluster do ONTAP, verifique se os nós estão íntegros e qualificados para participar do cluster e se o cluster está quórum. Você também deve verificar o status dos discos, agregados e volumes.

Verifique a integridade do cluster

Passos

1. Verifique se os nós do cluster estão online e estão qualificados para participar do cluster:

```
cluster show
```

Neste exemplo, o cluster está íntegro e todos os nós estão qualificados para participar do cluster.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

Se algum nó não for saudável ou não for elegível, verifique se há erros nos logs do EMS e tome medidas corretivas.

2. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

Entre `y` para continuar.

3. Verifique os detalhes de configuração para cada processo RDB.
   - A época do banco de dados relacional e as epochs do banco de dados devem corresponder para cada nó.
   - O mestre de quórum por anel deve ser o mesmo para todos os nós.

     Observe que cada anel pode ter um mestre de quórum diferente.

Para exibir este processo RDB…	Digite este comando…
Aplicação de gerenciamento	`cluster ring show -unitname mgmt`
Base de dados de localização de volume	`cluster ring show -unitname vldb`
Gerenciador de interface virtual	`cluster ring show -unitname vifmgr`
Daemon de gerenciamento SAN	`cluster ring show -unitname bcomd`

   Este exemplo mostra o processo do banco de dados de localização de volume:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

5. Se você estiver operando em um ambiente SAN, verifique se cada nó está em um quórum de SAN:

```
event log show  -severity informational -message-name scsiblade.*
```

A mensagem de evento scsipblade mais recente para cada nó deve indicar que o scsi-blade está em quórum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node        Severity       Event
---------------  ----------- -------------- ---------------------------
MM/DD/YYYY TIME  node0       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Informações relacionadas

"Administração do sistema"

Verifique a integridade do armazenamento

Depois de reverter ou fazer downgrade de um cluster, você deve verificar o status dos discos, agregados e volumes.

Passos

1. Verifique o status do disco:

Para verificar…	Faça isso…
Discos quebrados	a. Exibir todos os discos quebrados: `storage disk show -state broken` b. Remova ou substitua quaisquer discos quebrados.
Discos em manutenção ou reconstrução	a. Exiba todos os discos em estados de manutenção, pendentes ou reconstrução: `storage disk show -state maintenance`

Para verificar…	Faça isso…
pending	reconstructing ---- .. Aguarde até que a operação de manutenção ou reconstrução termine antes de prosseguir.

2. Verifique se todos os agregados estão online exibindo o estado do storage físico e lógico, incluindo agregados de storage:

```
storage aggregate show -state !online
```

Este comando exibe os agregados que estão *não* online. Todos os agregados devem estar online antes e depois de realizar uma grande atualização ou reversão.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verifique se todos os volumes estão online exibindo quaisquer volumes que estejam *não* online:

```
volume show -state !online
```

Todos os volumes devem estar online antes e depois de realizar uma grande atualização ou reversão.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verifique se não existem volumes inconsistentes:

```
volume show -is-inconsistent true
```

Consulte o artigo da base de dados de Conhecimento "Volume Mostrando WAFL inconsistente"sobre como resolver os volumes inconsistentes.

Informações relacionadas

"Gerenciamento de disco e agregado"

Verificação do acesso do cliente (SMB e NFS)

Para os protocolos configurados, teste o acesso de clientes SMB e NFS para verificar se o cluster está acessível.

Habilitar o switchover automático para configurações do MetroCluster após uma reversão do ONTAP

Depois de reverter uma configuração do ONTAP MetroCluster, você deve habilitar o switchover automático não planejado para garantir que a configuração do MetroCluster esteja totalmente operacional.

Passos

1. Ativar switchover não planejado automático:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

2. Valide a configuração do MetroCluster:

```
metrocluster check run
```

Ative e reverta LIFs para portas iniciais após uma reversão do ONTAP

Durante uma reinicialização, alguns LIFs podem ter sido migrados para suas portas de failover atribuídas. Depois de reverter um cluster do ONTAP, você deve habilitar e reverter quaisquer LIFs que não estejam em suas portas iniciais.

O comando de reversão da interface de rede reverte um LIF que não está atualmente em sua porta inicial de volta para sua porta inicial, desde que a porta inicial esteja operacional. A porta inicial de um LIF é especificada quando o LIF é criado; você pode determinar a porta inicial de um LIF usando o comando show de interface de rede.

Passos

1. Apresentar o estado de todas as LIFs:

```
network interface show
```

Este exemplo exibe o status de todas as LIFs de uma máquina virtual de storage (SVM).

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

Se algum LIFs for exibido com um status Admin de Status de Down ou com um status home de false, continue com a próxima etapa.

2. Ativar os LIFs de dados:

```
network interface modify {-role data} -status-admin up
```

3. Reverter LIFs para suas portas domésticas:

```
network interface revert *
```

4. Verifique se todos os LIFs estão em suas portas residenciais:

```
network interface show
```

Este exemplo mostra que todos os LIFs para SVM vs0 estão em suas portas domésticas.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0e
true
            data002      up/up    192.0.2.121/24     node0         e0f
true
            data003      up/up    192.0.2.122/24     node0         e2a
true
            data004      up/up    192.0.2.123/24     node0         e2b
true
            data005      up/up    192.0.2.124/24     node1         e0e
true
            data006      up/up    192.0.2.125/24     node1         e0f
true
            data007      up/up    192.0.2.126/24     node1         e2a
true
            data008      up/up    192.0.2.127/24     node1         e2b
true
8 entries were displayed.
```

Ative as políticas de cópia Snapshot após uma reversão do ONTAP

Depois de reverter para uma versão anterior do ONTAP, você deve habilitar as políticas de cópia Snapshot para começar a criar cópias snapshot novamente.

Você está rehabilitando as programações de instantâneos desativadas antes de reverter para uma versão anterior do ONTAP.

Passos

1. Habilite as políticas de cópia Snapshot para todas as SVMs de dados:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. Para cada nó, ative a política de cópia Snapshot do volume raiz:

```
run -node <node_name> vol options <volume_name> nosnap off
```

Verifique IPv6 entradas de firewall após uma reversão do ONTAP

Uma reversão de qualquer versão do ONTAP 9 pode resultar em entradas de firewall padrão IPv6 ausentes para alguns serviços em políticas de firewall. Você precisa verificar se as entradas de firewall necessárias foram restauradas para o sistema.

Passos

1. Verifique se todas as políticas de firewall estão corretas comparando-as com as políticas padrão:

```
system services firewall policy show
```

O exemplo a seguir mostra as políticas padrão:

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. Adicione manualmente quaisquer entradas padrão de firewall IPv6 ausentes criando uma nova política de firewall:

```
system services firewall policy create -policy <policy_name> -service
ssh -action allow -ip-list <ip_list>
```

3. Aplique a nova política ao LIF para permitir o acesso a um serviço de rede:

```
network interface modify -vserve <svm_name> -lif <lif_name> -firewall
-policy <policy_name>
```

Verifique as contas de usuário que podem acessar o processador de serviço depois de reverter para o ONTAP 9,8

No ONTAP 9.9.1 e posterior, o `-role` parâmetro para contas de usuário é alterado para `admin`. Se você criou contas de usuário no ONTAP 9,8 ou anterior, atualizou para o ONTAP 9.9.1 ou posterior e reverteu novamente para o ONTAP 9,8, o `-role` parâmetro será restaurado para seu valor original. Você deve verificar se os valores modificados são aceitáveis.

Durante a reversão, se a função de um usuário do SP tiver sido excluída, a mensagem "rbac.spuser.role.notfound" EMS será registrada.

Para obter mais informações, "Contas que podem acessar o SP"consulte .

Administração do cluster

Gerenciamento de clusters com o System Manager

Visão geral da administração com o System Manager

O System Manager é uma interface gráfica de gerenciamento baseada em HTML5 que permite usar um navegador da Web para gerenciar sistemas de storage e objetos de storage (como discos, volumes e camadas de storage) e executar tarefas comuns de gerenciamento relacionadas a sistemas de storage.

Os procedimentos nesta seção ajudam a gerenciar seu cluster com o System Manager no ONTAP 9.7 e versões posteriores.

- O Gerenciador do sistema está incluído no software ONTAP como um serviço da Web, habilitado por padrão e acessível por meio de um navegador.
- O nome do Gestor de sistema mudou a partir de ONTAP 9.6. Em ONTAP 9.5 e mais cedo foi chamado de OnCommand System Manager. Começando com o ONTAP 9.6 e posterior, ele é chamado de Gerenciador de sistema.
- Se você estiver usando o Gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e anterior), consulte "System Manager Classic (ONTAP 9 9,7.0 a 0)"

Com o System Manager Dashboard, é possível visualizar informações gerais sobre alertas e notificações importantes, a eficiência e a capacidade das camadas e volumes de storage, os nós disponíveis em um cluster, o status dos nós em um par de HA, as aplicações e objetos mais ativos e as métricas de performance de um cluster ou nó.

Com o System Manager, você pode executar muitas tarefas comuns, como as seguintes:

- Crie um cluster, configure uma rede e configure os detalhes de suporte para o cluster.
- Configure e gerencie objetos de storage, como discos, camadas locais, volumes, qtrees e cotas.
- Configurar protocolos, como SMB e NFS, e provisionar o compartilhamento de arquivos.
- Configurar protocolos como FC, FCoE, NVMe e iSCSI para acesso a bloco.
- Crie e configure componentes de rede, como sub-redes, domínios de broadcast, interfaces de dados e gerenciamento e grupos de interfaces.
- Configure e gerencie relacionamentos de espelhamento e cofre.
- Execute operações de gerenciamento de clusters, de nós de storage e de máquina virtual de armazenamento (VM de armazenamento).
- Crie e configure VMs de storage, gerencie objetos de storage associados a VMs de storage e gerencie serviços de VM de storage.
- Monitore e gerencie configurações de alta disponibilidade (HA) em um cluster.
- Configure os processadores de serviço para fazer login, gerenciar, monitorar e administrar remotamente o nó, independentemente do estado do nó.

Terminologia do System Manager

O Gerenciador do sistema usa terminologia diferente da CLI para algumas funcionalidades de chave do ONTAP.

- **Nível local** – um conjunto de unidades físicas de estado sólido ou unidades de disco rígido em que você armazena seus dados. Talvez você os conheça como agregados. Na verdade, se você usar a CLI do ONTAP, você ainda verá o termo *agregado* usado para representar um nível local.
- * Camada de nuvem* – armazenamento na nuvem usado pelo ONTAP quando você deseja ter alguns de seus dados fora do local por um dos vários motivos. Se você está pensando na parte da nuvem de um FabricPool, você já descobriu isso. E, se você estiver usando um sistema StorageGRID, sua nuvem pode não estar fora do local. (Uma experiência semelhante à nuvem no local é chamada de *nuvem privada*.)
- **Storage VM** – uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um *SVM* ou um *vserver*.
- **Interface de rede** - um endereço e propriedades atribuídos a uma porta de rede física. Você pode saber isso como uma *interface lógica (LIF)*.
- **Pausa** - uma ação que pára as operações. Antes do ONTAP 9.8, você pode ter se referido a *quiesce* em outras versões do Gerenciador de sistema.

Use o System Manager para acessar um cluster

Se você preferir usar uma interface gráfica em vez da interface de linha de comando (CLI) para acessar e gerenciar um cluster, você pode fazer isso usando o Gerenciador de sistema, que está incluído no ONTAP como serviço da Web, é habilitado por padrão e acessível usando um navegador.

> A partir do ONTAP 9.12,1, o Gerenciador de sistema é totalmente integrado ao BlueXP .
>
> Com o BlueXP , você pode gerenciar sua infraestrutura multicloud híbrida a partir de um único painel de controle enquanto mantém o já conhecido painel do System Manager.
>
> "Integração do System Manager com o BlueXP "Consulte .

Sobre esta tarefa

Você pode usar uma interface de rede de gerenciamento de cluster (LIF) ou uma interface de rede de gerenciamento de nós (LIF) para acessar o System Manager. Para acesso ininterrupto ao System Manager, você deve usar uma interface de rede de gerenciamento de cluster (LIF).

Antes de começar

- Você deve ter uma conta de usuário de cluster configurada com a função "'admin'" e os tipos de aplicativo "'http'" e "'console'".
- Você deve ter ativado cookies e dados do site no navegador.

Passos

1. Aponte o navegador da Web para o endereço IP da interface de rede de gerenciamento de cluster:
    - Se você estiver usando IPv4: **`https://cluster-mgmt-LIF`**
    - Se você estiver usando IPv6: **`https://[cluster-mgmt-LIF]`**

Apenas o HTTPS é suportado para acesso ao navegador do System Manager.

Se o cluster usar um certificado digital autoassinado, o navegador pode exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela autoridade de certificação (CA) no cluster para autenticação do servidor.

2. **Opcional:** se você configurou um banner de acesso usando a CLI, leia a mensagem exibida na caixa de diálogo **Aviso** e escolha a opção necessária para continuar.

   Esta opção não é suportada em sistemas nos quais a autenticação SAML (Security Assertion Markup Language) está ativada.

   - Se você não quiser continuar, clique em **Cancelar** e feche o navegador.
   - Se pretender continuar, clique em **OK** para navegar para a página de início de sessão do Gestor do sistema.

3. Faça login no System Manager usando as credenciais de administrador de cluster.

   A partir do ONTAP 9.11,1, quando você faz login no Gerenciador de sistema, você pode especificar a localidade. A localidade especifica certas configurações de localização, como idioma, moeda, formato de hora e data e configurações semelhantes. Para o ONTAP 9.10,1 e anteriores, o local para o Gerenciador de sistema é detetado no navegador. Para alterar a localidade do System Manager, é necessário alterar a localidade do navegador.

4. **Opcional**: Começando com ONTAP 9.12,1, você pode especificar sua preferência para a aparência do Gerenciador de sistema:
   a. No canto superior direito do System Manager, clique em para gerir as opções do utilizador.
   b. Posicione o interrutor de alternância **tema do sistema** de acordo com sua preferência:

Alternar a posição	Definição de aspeto
(esquerda)	Tema claro (Fundo claro com texto escuro)
SO (centro)	Padrão para a preferência de tema que foi definida para os aplicativos do sistema operacional (geralmente a configuração de tema para o navegador que é usado para acessar o System Manager).
(direita)	Tema escuro (fundo escuro com texto claro)

Informações relacionadas

"Gerenciando o acesso a serviços da Web"

"Acessando os arquivos de log, despejo de núcleo e MIB de um nó usando um navegador da Web"

Ative novos recursos adicionando chaves de licença

Em versões anteriores ao ONTAP 9.10,1, os recursos do ONTAP são habilitados com chaves de licença e os recursos no ONTAP 9.10,1 e posteriores são habilitados com um

arquivo de licença do NetApp. Você pode adicionar chaves de licença e arquivos de licença do NetApp usando o Gerenciador do sistema.

A partir do ONTAP 9.10,1, você usa o Gerenciador de sistema para instalar um arquivo de licença do NetApp para habilitar vários recursos licenciados de uma só vez. O uso de um arquivo de licença do NetApp simplifica a instalação de licenças porque você não precisa mais adicionar chaves de licença de recursos separadas. Transfira o ficheiro de licença do NetApp a partir do site de suporte da NetApp.

Se você já tiver chaves de licença para alguns recursos e estiver atualizando para o ONTAP 9.10,1, poderá continuar usando essas chaves de licença.

Passos

1. Selecione **Cluster > Settings**.
2. Em **licenças**, → selecione .
3. Selecione **Procurar**. Escolha o arquivo de licença do NetApp que você baixou.
4. Se você tiver chaves de licença que deseja adicionar, selecione **usar chaves de licença de 28 carateres** e insira as chaves.

Faça download de uma configuração de cluster

A partir do ONTAP 9.11,1, você pode usar o Gerenciador do sistema para baixar alguns detalhes de configuração sobre o cluster e seus nós. Essas informações podem ser usadas para gerenciamento de inventário, substituição de hardware e atividades de ciclo de vida. Essas informações são especialmente úteis para sites que não enviam dados do AutoSupport (ASUP).

Os detalhes de configuração do cluster incluem o nome do cluster, a versão do cluster ONTAP, a LIF de gerenciamento de cluster, o volume e as contagens de LIF.

Os detalhes de configuração do nó incluem o nome do nó, o número de série do sistema, a ID do sistema, o modelo do sistema, a versão do ONTAP, as informações de MetroCluster, as informações de rede do SP/BMC e as informações de configuração de criptografia.

Passos

1. Clique em **Cluster > Overview**.
2. Clique 

para exibir o menu suspenso.
3. Selecione **Download Configuration**.
4. Selecione os pares HA e clique em **Download**.

   A configuração é transferida como uma folha de cálculo do Excel.

   - A primeira folha contém detalhes do cluster.
   - As outras folhas contêm detalhes do nó.

Atribua tags a um cluster

A partir do ONTAP 9.14,1, você pode usar o Gerenciador de sistema para atribuir tags a um cluster para identificar objetos como pertencentes a uma categoria, como projetos ou

centros de custo.

Sobre esta tarefa

Pode atribuir uma etiqueta a um cluster. Primeiro, você precisa definir e adicionar a tag. Em seguida, você também pode editar ou excluir a tag.

As tags podem ser adicionadas quando você cria um cluster ou podem ser adicionadas mais tarde.

Você define uma tag especificando uma chave e associando um valor a ela usando o formato "chave:valor". Por exemplo: "dept:Engineering" ou "location:san-jose".

O seguinte deve ser considerado quando você cria tags:

- As chaves têm um comprimento mínimo de um caractere e não podem ser nulas. Os valores podem ser nulos.
- Uma chave pode ser emparelhada com vários valores separando os valores com uma vírgula, por exemplo, "'location:san-Jose,toronto'"
- As tags podem ser usadas para vários recursos.
- As teclas devem começar com uma letra minúscula.

Passos

Para gerenciar tags, execute as seguintes etapas:

1. No System Manager, clique em **Cluster** para visualizar a página de visão geral.

   As tags estão listadas na seção **Tags**.

2. Clique em **Gerenciar tags** para modificar tags existentes ou adicionar novas.

   Você pode adicionar, editar ou excluir as tags.

Para executar esta ação…	Execute estas etapas…
Adicione uma tag	a. Clique em **Add Tag**. b. Especifique uma chave e seu valor ou valores (separe vários valores com vírgulas). c. Clique em **Salvar**.
Edite uma tag	a. Modifique o conteúdo nos campos **Key** e **values (opcional)**. b. Clique em **Salvar**.
Excluir uma tag	a. Clique ao lado da tag que você deseja excluir.

Visualizar e enviar casos de suporte

A partir do ONTAP 9.9,1, é possível visualizar casos de suporte do consultor digital do Active IQ (também conhecido como consultor digital) associados ao cluster. Você também pode copiar os detalhes do cluster de que precisa para enviar um novo caso de

suporte no site de suporte da NetApp. A partir do ONTAP 9.10,1, você pode ativar o Registro de telemetria, o que ajuda a equipe de suporte a solucionar problemas.

Para receber alertas sobre atualizações de firmware, você deve estar registrado no Active IQ Unified Manager. "Recursos de documentação do Active IQ Unified Manager"Consulte a .

Passos

1. No System Manager, selecione **Support**.

   É apresentada uma lista de casos de suporte abertos associados a este cluster.

2. Clique nos seguintes links para executar procedimentos:
   - **Número do caso**: Veja detalhes sobre o caso.
   - **Vá para o site de suporte da NetApp**: Navegue até a página **My AutoSupport** no site de suporte da NetApp para ver os artigos da base de conhecimento ou enviar um novo caso de suporte.
   - **Exibir Meus casos**: Navegue até a página **Meus casos** no site de suporte da NetApp.
   - **Exibir Detalhes do cluster**: Visualize e copie informações que você precisará quando enviar um novo caso.

Ativar o registo de telemetria

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para ativar o Registro de telemetria. Quando o Registro de telemetria é permitido, as mensagens registradas pelo System Manager recebem um identificador de telemetria específico que indica o processo exato que acionou a mensagem. Todas as mensagens que são emitidas relacionadas a esse processo têm o mesmo identificador, que consiste no nome do fluxo de trabalho operacional e um número (por exemplo, "add-volume-1941290").

Se você tiver problemas de desempenho, poderá ativar o Registro de telemetria, o que permite que a equipe de suporte identifique mais facilmente o processo específico para o qual uma mensagem foi emitida. Quando identificadores de telemetria são adicionados às mensagens, o arquivo de log é apenas ligeiramente aumentado.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Configurações da IU**, clique na caixa de seleção **permitir Registro de telemetria**.

Gerencie o limite máximo de capacidade de uma VM de storage no System Manager

A partir do ONTAP 9.13,1, você pode usar o Gerenciador do sistema para habilitar um limite máximo de capacidade para uma VM de storage e definir um limite para acionar alertas quando o storage usado atinge uma determinada porcentagem da capacidade máxima.

Habilite um limite máximo de capacidade para uma VM de storage

A partir do ONTAP 9.13,1, é possível especificar a capacidade máxima que pode ser alocada para todos os volumes em uma VM de storage. É possível habilitar a capacidade máxima quando você adiciona uma VM de storage ou quando edita uma VM de storage existente.

Passos

1. Selecione **Storage** > **Storage VMs**.
2. Execute um dos seguintes procedimentos:
   - Para adicionar uma VM de armazenamento, clique + Add em .
   - Para editar uma VM de armazenamento, clique ⋮ ao lado do nome da VM de armazenamento e, em seguida, clique em **Editar**.
3. Introduza ou modifique as definições da VM de armazenamento e selecione a caixa de verificação "Ativar limite máximo de capacidade".
4. Especifique o tamanho máximo da capacidade.
5. Especifique a porcentagem da capacidade máxima que você deseja usar como limite para acionar alertas.
6. Clique em **Salvar**.

Edite o limite máximo de capacidade de uma VM de armazenamento

A partir do ONTAP 9.13,1, você pode editar o limite máximo de capacidade de uma VM de armazenamento existente, se já houvero limite máximo de capacidade foi ativado.

Passos

1. Selecione **Storage** > **Storage VMs**.
2. Clique ⋮ ao lado do nome da VM de armazenamento e, em seguida, clique em **Editar**.

   A caixa de verificação intitulada "Ativar limite máximo de capacidade" já está marcada.
3. Execute um dos seguintes passos:

Ação	Passos
Desative o limite máximo de capacidade	1. Desmarque a caixa de seleção. 2. Clique em **Salvar**.
Modifique o limite máximo de capacidade	1. Especifique o novo tamanho máximo da capacidade. (Não é possível especificar um tamanho menor do que o espaço já alocado na VM de armazenamento.) 2. Especifique a nova porcentagem da capacidade máxima que você deseja usar como limite para acionar alertas. 3. Clique em **Salvar**.

Informações relacionadas

- "Exibir o limite máximo de capacidade de uma VM de storage"
- "Medições de capacidade no System Manager"
- "Gerenciar limites de capacidade do SVM"

Monitorar a capacidade no System Manager

Com o System Manager, você pode monitorar quanto de capacidade de storage foi usada e quanto ainda está disponível para um cluster, uma camada local ou uma VM de storage.

Com cada versão do ONTAP, o Gerenciador de sistemas fornece informações de monitoramento de capacidade mais robustas:

- A partir do ONTAP 9.10,1, o Gerenciador de sistemas permite visualizar dados históricos sobre a capacidade e projeções do cluster sobre a quantidade de capacidade que será usada ou disponível no futuro. Também é possível monitorar a capacidade de camadas e volumes locais.
- A partir do ONTAP 9.12,1, o Gerenciador de sistema exibe a quantidade de capacidade comprometida de um nível local.
- A partir do ONTAP 9.13,1, é possível habilitar um limite máximo de capacidade para uma VM de storage e definir um limite para acionar alertas quando o storage usado atinge uma determinada porcentagem da capacidade máxima.

As medições da capacidade utilizada são apresentadas de forma diferente, dependendo da versão do ONTAP. Saiba mais em "Medições de capacidade no System Manager".

Exibir a capacidade de um cluster

Pode visualizar as medições de capacidade de um cluster no painel de instrumentos no System Manager.

Antes de começar

Para exibir dados relacionados à capacidade na nuvem, você precisa ter uma conta no Digital Advisor e estar conetado.

Passos

1. No System Manager, clique em **Dashboard**.
2. Na seção **capacidade**, você pode ver o seguinte:
    - Capacidade total utilizada do cluster
    - Capacidade total disponível do cluster
    - Percentagens de capacidade utilizada e disponível.
    - Relação de redução de dados.
    - Quantidade de capacidade usada na nuvem.
    - Histórico de uso da capacidade.
    - Projeção do uso da capacidade

    No System Manager, as representações de capacidade não são responsáveis pelas capacidades da camada de storage raiz (agregado).

3. Clique no gráfico para ver mais detalhes sobre a capacidade do cluster.

    As medições de capacidade são apresentadas em duas cartas de barras:

- O gráfico superior exibe a capacidade física: O tamanho do espaço físico usado, reservado e disponível.
- O gráfico inferior exibe a capacidade lógica: O tamanho dos dados do cliente, as cópias Snapshot e os clones e o espaço lógico total usado.

Abaixo dos gráficos de barras estão as medições para redução de dados:

- Taxa de redução de dados somente para os dados do cliente (cópias e clones do Snapshot não estão incluídos).
- Relação geral de redução de dados.

Para obter mais informações, "Medições de capacidade no System Manager"consulte .

Visualizar a capacidade de um nível local

É possível visualizar detalhes sobre a capacidade das camadas locais. A partir do ONTAP 9.12,1, a visualização **capacidade** também inclui a quantidade de capacidade comprometida de um nível local, permitindo que você determine se precisa adicionar capacidade ao nível local para acomodar a capacidade comprometida e evitar ficar sem espaço livre.

Passos

1. Clique em **armazenamento > camadas**.
2. Selecione o nome do nível local.
3. Na página **Visão geral**, na seção **capacidade**, a capacidade é mostrada em um gráfico de barras com três medidas:
   - Capacidade utilizada e reservada
   - Capacidade disponível
   - Capacidade comprometida (começando com ONTAP 9.12,1)
4. Clique no gráfico para ver detalhes sobre a capacidade do nível local.

   As medições de capacidade são apresentadas em duas cartas de barras:

   - O gráfico de barras superior exibe a capacidade física: O tamanho do espaço físico usado, reservado e disponível.
   - O gráfico de barras inferior exibe a capacidade lógica: O tamanho dos dados do cliente, as cópias Snapshot e os clones e o total de espaço lógico usado.

   Abaixo dos gráficos de barras estão as relações de medição para redução de dados:

   - Taxa de redução de dados somente para os dados do cliente (cópias e clones do Snapshot não estão incluídos).
   - Relação geral de redução de dados.

Para obter mais informações, "Medições de capacidade no System Manager"consulte .

Ações opcionais

- Se a capacidade comprometida for maior que a capacidade do nível local, você pode considerar adicionar capacidade ao nível local antes que ele fique sem espaço livre. "Adicionar capacidade a um nível local (adicionar discos a um agregado)"Consulte .

- Você também pode exibir o armazenamento que volumes específicos usam no nível local selecionando a guia **volumes**.

Visualizar a capacidade dos volumes em uma VM de storage

Você pode ver quanto storage é usado pelos volumes em uma VM de storage e quanto de capacidade ainda está disponível. A medição total do armazenamento usado e disponível é chamada de "capacidade entre volumes".

Passos

1. Selecione **Storage** > **Storage VMs**.
2. Clique no nome da VM de armazenamento.
3. Role até a seção **Capacity**, que mostra um gráfico de barras com as seguintes medidas:
   - **Físico usado**: Soma do armazenamento físico usado em todos os volumes nesta VM de armazenamento.
   - **Disponível**: Soma da capacidade disponível em todos os volumes nesta VM de armazenamento.
   - **Uso lógico**: Soma do armazenamento lógico usado em todos os volumes nesta VM de armazenamento.

Para obter mais detalhes sobre as medições, "Medições de capacidade no System Manager"consulte .

Exibir o limite máximo de capacidade de uma VM de storage

A partir do ONTAP 9.13,1, é possível visualizar o limite máximo de capacidade de uma VM de armazenamento.

Antes de começar

Você deve "Ative o limite máximo de capacidade de uma VM de storage" antes de poder visualizá-lo.

Passos

1. Selecione **Storage** > **Storage VMs**.

   Pode visualizar as medições da capacidade máxima de duas formas:

   - Na linha da VM de armazenamento, veja a coluna **capacidade máxima** que contém um gráfico de barras que mostra a capacidade usada, a capacidade disponível e a capacidade máxima.
   - Clique no nome da VM de armazenamento. Na guia **Visão geral**, role para ver os valores limite de capacidade máxima, capacidade alocada e capacidade de alerta na coluna esquerda.

Informações relacionadas

- "Edite o limite máximo de capacidade de uma VM de armazenamento"
- "Medições de capacidade no System Manager"

Veja as configurações do hardware para determinar problemas

A partir do ONTAP 9.8, você pode usar o Gerenciador de sistema para visualizar a configuração do hardware na rede e determinar a integridade dos sistemas de hardware e configurações de cabeamento.

Passos

Para exibir configurações de hardware, execute as seguintes etapas:

1. No System Manager, selecione **Cluster > hardware**.
2. Passe o Mouse sobre os componentes para ver o status e outros detalhes.

   Você pode visualizar vários tipos de informações:

   - Informações sobre controladores
   - Informações sobre compartimentos de disco
   - Informações sobre switches de armazenamento
3. A partir do ONTAP 9.12,1, é possível visualizar informações de cabeamento no Gerenciador de sistemas. Clique na caixa de seleção **Mostrar cabos** para visualizar o cabeamento e, em seguida, passe o Mouse sobre um cabo para exibir suas informações de conetividade.
   - Informações sobre cabeamento

Informações sobre controladores

Você pode ver o seguinte:

Nós

- Pode ver as vistas dianteira e traseira.
- Para modelos com um compartimento de disco interno, você também pode exibir o layout do disco na exibição frontal.
- Você pode visualizar as seguintes plataformas:

Plataforma	Suportado no Gerenciador de sistema na versão ONTAP…							
	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8 (apenas modo de pré-visualização)
AFF A70	Sim							
AFF A90	Sim							
AFF A1K	Sim							
AFF A150	Sim	Sim	Sim					
AFF A220	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AFF A250	Sim	Sim	Sim	Sim	Sim	Sim	Sim	
AFF A300	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AFF A320	Sim	Sim	Sim	Sim	Sim	Sim	Sim	
AFF A400	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AFF A700	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AFF A700s	Sim	Sim	Sim	Sim	Sim	Sim	Sim	
AFF A800	Sim	Sim	Sim	Sim	Sim	Sim	Sim	

AFF C190	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AFF C250	Sim	Sim	Sim	Sim e n.o 42;	Sim e n.o 42;	Sim e n.o 42;		
AFF C400	Sim	Sim	Sim	Sim e n.o 42;	Sim e n.o 42;	Sim e n.o 42;		
AFF C800	Sim	Sim	Sim	Sim e n.o 42;	Sim e n.o 42;	Sim e n.o 42;		
ASA A150	Sim	Sim	Sim					
ASA A250	Sim	Sim	Sim					
ASA A400	Sim	Sim	Sim					
ASA A800	Sim	Sim	Sim					
ASA A900	Sim	Sim	Sim					
ASA C250	Sim	Sim	Sim					
ASA C400	Sim	Sim	Sim					
ASA C800	Sim	Sim	Sim					
FAS500f	Sim	Sim	Sim	Sim	Sim	Sim	Sim	
FAS2720	Sim	Sim	Sim	Sim	Sim			
FAS2750	Sim	Sim	Sim	Sim	Sim			
FAS8300	Sim	Sim	Sim	Sim	Sim			
FAS8700	Sim	Sim	Sim	Sim	Sim			

FAS9000	Sim	Sim	Sim	Sim	Sim			
FAS9500	Sim	Sim	Sim	Sim	Sim			

Portas

- Você verá uma porta realçada em vermelho se estiver para baixo.
- Ao passar o Mouse sobre a porta, você pode exibir o status de uma porta e outros detalhes.
- Não é possível exibir portas de console.

  Notas:

  - Para o ONTAP 9.10,1 e versões anteriores, você verá as portas SAS destacadas em vermelho quando elas estiverem desativadas.
  - A partir do ONTAP 9.11,1, você verá as portas SAS destacadas em vermelho somente se estiverem em um estado de erro ou se uma porta cabeada que está sendo usada ficar offline. As portas aparecem em branco se estiverem off-line e sem fio.

FRUs

As informações sobre FRUs são exibidas somente quando o estado de uma FRU não é ideal.

- PSUs com falha em nós ou chassi.
- Altas temperaturas detetadas nos nós.
- Ventiladores com falha nos nós ou no chassi.

Placas adaptadoras

- Os cartões com campos de número de peça definidos são exibidos nos slots se os cartões externos tiverem sido inseridos.
- As portas são exibidas nos cartões.
- Para um cartão suportado, pode visualizar imagens desse cartão. Se a placa não estiver na lista de números de peça suportados, um gráfico genérico será exibido.

Informações sobre compartimentos de disco

Você pode ver o seguinte:

Compartimentos de disco

- Pode apresentar as vistas dianteira e traseira.
- Você pode ver os seguintes modelos de compartimento de disco:

Se o seu sistema estiver em execução…	Então você pode usar o Gerenciador do sistema para exibir…
ONTAP 9.9,1 e posterior	Todas as prateleiras que *não* foram designadas como "fim de serviço" ou "fim de disponibilidade"
ONTAP 9,8	DS4243, DS4486, DS212C, DS2246, DS224C E NS224

Portas do compartimento

- Você pode exibir o status da porta.
- Você pode exibir informações de porta remota se a porta estiver conetada.

FRUs de gaveta

- As informações de falha da PSU são exibidas.

Informações sobre switches de armazenamento

Você pode ver o seguinte:

Interrutores de armazenamento

- O visor mostra os switches que atuam como switches de storage usados para conectar gavetas a nós.
- A partir do ONTAP 9.9,1, o Gerenciador de sistema exibe informações sobre um switch que atua como um switch de storage e um cluster, que também pode ser compartilhado entre nós de um par de HA.
- As seguintes informações são exibidas:
  - Mudar nome
  - Endereço IP
  - Número de série
  - Versão de SNMP
  - Versão do sistema
- Pode visualizar os seguintes modelos de comutador de armazenamento:

Se o seu sistema estiver em execução…	Então você pode usar o Gerenciador do sistema para exibir…
ONTAP 9.11,1 ou posterior	Cisco Nexus 3232C Cisco Nexus 9336C-FX2P Mellanox SN2100
ONTAP 9.9,1 e 9.10.1	Cisco Nexus 3232C Cisco 9336C-FX2
ONTAP 9,8	Cisco Nexus 3232C

Portas do switch de armazenamento

- As seguintes informações são exibidas:
  - Nome de identidade
  - Índice de identidade
  - Estado
  - Ligação remota
  - Outros detalhes

Informações sobre cabeamento

A partir do ONTAP 9.12,1, você pode visualizar as seguintes informações de cabeamento:

- **Cabeamento** entre controladoras, switches e gavetas quando não forem usadas pontes de storage
- **Conetividade** que mostra os IDs e endereços MAC das portas em qualquer extremidade do cabo

Gerencie nós usando o System Manager

Usando o System Manager, você pode adicionar nós a um cluster e renomeá-los. Você também pode reinicializar, assumir e devolver nós.

Adicionar nós a um cluster

Você pode aumentar o tamanho e as funcionalidades do cluster adicionando novos nós.

Antes de começar

Você já deve ter cabeado os novos nós para o cluster.

Sobre esta tarefa

Existem processos separados para trabalhar com o System Manager no ONTAP 9.7 ou ONTAP 9.8 e posterior.

Procedimento ONTAP 9.8 e posterior

Adicionando nós a um cluster com o System Manager (ONTAP 9.8 e posterior)

Passos

1. Selecione **Cluster > Overview**.

   Os novos controladores são mostrados como nós conetados à rede do cluster, mas não estão no cluster.

2. Selecione **Adicionar**.
   - Os nós são adicionados ao cluster.
   - O armazenamento é alocado implicitamente.

Procedimento ONTAP 9.7

Adicionando nós a um cluster com o Gerenciador de sistema (ONTAP 9.7)

Passos

1. Selecione **(retornar à versão clássica)**.
2. Selecione **Configurações > expansão de cluster**.

   O System Manager descobre automaticamente os novos nós.

3. Selecione **mudar para a nova experiência**.
4. Selecione **Cluster > Overview** para visualizar os novos nós.

Encerre, reinicie ou edite o processador de serviço

Quando você reinicializar ou encerrar um nó, o parceiro de HA executa automaticamente um takeover.

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para encerrar e reinicializar um nó. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Passos

1. Selecione **Cluster > Overview**.
2. Em **nós**, selecione .

3. Selecione o nó e, em seguida, selecione **Desligar**, **Reiniciar** ou **Editar processador de serviço**.

   Se um nó foi reinicializado e está aguardando a giveback, a opção **Giveback** também está disponível.

   Se selecionar **Editar processador de serviço**, pode escolher **Manual** para introduzir o endereço IP, a máscara de sub-rede e o gateway, ou pode escolher **DHCP** para a configuração dinâmica do anfitrião.

Mudar o nome dos nós

A partir do ONTAP 9.14,1, você pode renomear um nó na página de visão geral do cluster.

> Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para renomear um nó. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Passos

1. Selecione **Cluster**. A página de visão geral do cluster é exibida.
2. Role para baixo até a seção **nodes**.
3. Ao lado do nó que você deseja renomear, selecione ⋮ e selecione **Renomear**.
4. Modifique o nome do nó e selecione **Renomear**.

Gerenciamento de licenças

Visão geral do licenciamento do ONTAP

Uma licença é um Registro de um ou mais direitos de software. A partir do ONTAP 9.10,1, todas as licenças são entregues como um arquivo de licença NetApp (NLF), que é um único arquivo que permite vários recursos. A partir de maio de 2023, todos os sistemas AFF (Série A e série C) e FAS são vendidos com o pacote de software ONTAP One ou o pacote de software ONTAP base e, a partir de junho de 2023, todos os sistemas ASA são vendidos com o ONTAP One para SAN. Cada pacote de software é fornecido como um único NLF, substituindo os pacotes NLF separados introduzidos pela primeira vez no ONTAP 9.10,1.

Licenças incluídas no ONTAP One

O ONTAP One contém todas as funcionalidades licenciadas disponíveis. Ele contém uma combinação do conteúdo do antigo pacote Core, do pacote Data Protection, do pacote Security and Compliance, do pacote Hybrid Cloud e do pacote Encryption, conforme mostrado na tabela. A criptografia não está disponível em países restritos.

Nome antigo do pacote	Chaves ONTAP incluídas

Pacote básico	FlexClone
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI
	NVMe-of
Pacote de segurança e conformidade	Proteção autônoma contra ransomware
	MTKM
	SnapLock
Pacote de proteção de dados	SnapMirror (assíncrono, síncrono, continuidade dos negócios)
	SnapCenter
	SnapMirror S3 para alvos NetApp
Pacote de nuvem híbrida	Nuvem da SnapMirror
	SnapMirror S3 para alvos não-NetApp
Pacote de criptografia	Criptografia de volume do NetApp
	Módulo Plataforma confiável

Licenças não incluídas no ONTAP One

O ONTAP One não inclui nenhum dos serviços fornecidos em nuvem da NetApp, incluindo o seguinte:

- Disposição em camadas do BlueXP (anteriormente conhecida como disposição em camadas na nuvem)
- Cloud Insights
- Backup BlueXP
- Governança de dados

ONTAP One para sistemas existentes

Se você tiver sistemas existentes que estão atualmente sob suporte do NetApp, mas não foram atualizados para o ONTAP One, as licenças existentes nesses sistemas ainda serão válidas e continuarão funcionando conforme esperado. Por exemplo, se a licença SnapMirror já estiver instalada em sistemas existentes, não será necessário atualizar para o ONTAP One para obter uma nova licença SnapMirror. No entanto, se você não tiver uma licença SnapMirror instalada em um sistema existente, a única maneira de obter essa licença é atualizar para o ONTAP One por uma taxa adicional.

A partir de junho de 2023, os sistemas ONTAP que usam chaves de licença de 28 carateres também podem "Atualize para o pacote de compatibilidade ONTAP One ou ONTAP base".

Licenças incluídas no ONTAP base

O ONTAP base é um pacote de software opcional que é uma alternativa ao ONTAP One para sistemas ONTAP. Ele é para casos de uso específicos em que não são necessárias tecnologias de proteção de dados, como o SnapMirror e o SnapCenter, bem como recursos de segurança, como o Autonomous ransomware, como sistemas não produtivos para ambientes dedicados de teste ou desenvolvimento. Licenças adicionais

não podem ser adicionadas ao ONTAP base. Se você quiser licenças adicionais, como o SnapMirror, você deve atualizar para o ONTAP One.

Nome antigo do pacote	Chaves ONTAP incluídas
Pacote básico	FlexClone
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI
	NVMe-of
Pacote de criptografia	Criptografia de volume do NetApp
	Módulo Plataforma confiável

Licenças incluídas no ONTAP One para SAN

O ONTAP One para SAN está disponível para sistemas ASA da série A e série C. Este é o único pacote de software disponível para SAN. O ONTAP One para SAN contém as seguintes licenças:

Chaves ONTAP incluídas
FlexClone
SnapRestore
FC, iSCSI
NVMe-of
MTKM
SnapLock
SnapMirror (assíncrono, síncrono, continuidade dos negócios)
SnapCenter
Nuvem da SnapMirror
Criptografia de volume do NetApp
Módulo Plataforma confiável

Outros métodos de entrega de licenças

No ONTAP 8,2 até ONTAP 9.9,1, as chaves de licença são entregues como strings de 28 carateres, e há uma chave por recurso ONTAP. Você usa a CLI do ONTAP para instalar chaves de licença se estiver usando o ONTAP 8,2 através do ONTAP 9.9,1.

> O ONTAP 9.10,1 suporta a instalação de chaves de licença de 28 carateres usando o Gerenciador do sistema ou a CLI. No entanto, se uma licença NLF for instalada para um recurso, você não poderá instalar uma chave de licença de 28 carateres sobre o arquivo de licença NetApp para o mesmo recurso. Para obter informações sobre como instalar NLFs ou chaves de licença usando o System Manager, "Instalar licenças ONTAP"consulte .

Informações relacionadas

"Como obter uma licença ONTAP One quando o sistema já tiver NLFs"

"Como verificar os direitos do software ONTAP e as chaves de licença relacionadas usando o site de suporte"

"NetApp: Status de risco de direito do ONTAP"

Faça download dos arquivos de licença do NetApp (NLF) no site de suporte da NetApp

Se o seu sistema estiver executando o ONTAP 9.10,1 ou posterior, você poderá atualizar os arquivos de licença do pacote em sistemas existentes baixando o NLF para ONTAP One ou núcleo ONTAP a partir do site de suporte da NetApp.

As licenças SnapMirror Cloud e SnapMirror S3 não estão incluídas no ONTAP One. Eles fazem parte do pacote de compatibilidade do ONTAP One, que você pode obter gratuitamente se você tiver o ONTAP One e "solicite separadamente"o .

Passos

Você pode baixar arquivos de licença do ONTAP One para sistemas com pacotes de arquivos de licença do NetApp existentes e para sistemas com chaves de licença de 28 carateres que foram convertidas em arquivos de licença do NetApp em sistemas executando o ONTAP 9.10,1 e posterior. Por uma taxa, você também pode atualizar os sistemas do ONTAP base para o ONTAP One.

Atualizar NLF existente

1. Entre em Contato com sua equipe de vendas da NetApp e solicite o pacote de arquivos de licença que você deseja atualizar ou converter (por exemplo, ONTAP base para ONTAP One ou pacote básico e pacote de proteção de dados para ONTAP One).

   Quando a sua solicitação for processada, você receberá um e-mail da NetApp.com com com o assunto "notificação de Licenciamento de Software da NetApp para O número [número ASSIM]" e o e-mail incluirá um anexo em PDF que inclui o número de série da sua licença.

2. Inicie sessão no "Site de suporte da NetApp".
3. Selecione **sistemas > licenças de software**.
4. No menu, escolha **número de série**, insira o número de série que recebeu e clique em **Nova Pesquisa**.
5. Localize o pacote de licenças que você deseja converter.
6. Clique em **Get NetApp License File** para cada pacote de licença e baixe os NLFs quando estiverem disponíveis.
7. "Instale" O arquivo ONTAP One.

Atualize o NLF convertido da chave de licença

1. Inicie sessão no "Site de suporte da NetApp".
2. Selecione **sistemas > licenças de software**.
3. No menu, escolha **número de série**, insira o número de série do sistema e clique em **Nova Pesquisa**.
4. Localize a licença que você deseja converter e, na coluna **elegibilidade**, clique em **verificar**.
5. No **formulário de elegibilidade**, clique em **Generate licenses for 9,10.x and later**.
6. Feche o **Verifique o formulário de elegibilidade**.

   Você precisará esperar pelo menos 2 horas para que as licenças sejam geradas.

7. Repita os passos 1 a 3.
8. Localize a licença ONTAP One, clique em **obter ficheiro de licença NetApp** e escolha o método de entrega.
9. "Instale" O arquivo ONTAP One.

Instalar licenças NetApp no ONTAP

Você pode instalar arquivos de licença do NetApp (NLFs) e chaves de licença usando o Gerenciador de sistema, que é o método preferido para instalar NLFs, ou você pode usar a CLI do ONTAP para instalar chaves de licença. No ONTAP 9.10,1 e posterior, os recursos são habilitados com um arquivo de licença NetApp e, em versões anteriores ao ONTAP 9.10,1, os recursos do ONTAP são habilitados com chaves de licença.

Passos

Se você já tiver "Arquivos de licença do NetApp baixados"ou chaves de licença, você pode usar o Gerenciador do sistema ou a CLI do ONTAP para instalar NLFs e chaves de licença de 28 carateres.

Gestor do sistema - ONTAP 9.8 e posterior

1. Selecione **Cluster > Settings**.
2. Em **licenças**, → selecione .
3. Selecione **Procurar**. Escolha o arquivo de licença do NetApp que você baixou.
4. Se você tiver chaves de licença que deseja adicionar, selecione **usar chaves de licença de 28 carateres** e insira as chaves.

Gestor do sistema - ONTAP 9.7 e anteriores

1. Selecione **Configuração > Cluster > licenças**.
2. Em **licenças**, → selecione .
3. Na janela **Pacotes**, clique em **Adicionar**.
4. Na caixa de diálogo **Adicionar pacotes de licença**, clique em **escolher arquivos** para selecionar o arquivo de licença do NetApp que você baixou e clique em **Adicionar** para carregar o arquivo para o cluster.

CLI

1. Adicione uma ou mais chaves de licença:

   ```
   system license add
   ```

   O exemplo a seguir instala licenças do nó local "/mroot/etc/lic_file" se o arquivo existir neste local:

   ```
   cluster1::> system license add -use-license-file true
   ```

   O exemplo a seguir adiciona uma lista de licenças com as chaves AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBBB
   ```

   Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/system-license-add.html[`system license add` em referência de comando ONTAP.

Gerenciar licenças do ONTAP

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para exibir e gerenciar licenças instaladas no sistema, incluindo a exibição do número de série da licença, a verificação do status de uma licença e a remoção de uma licença.

Ver detalhes sobre uma licença

Passos

A forma como você visualiza detalhes sobre uma licença depende da versão do ONTAP que você está usando e se você usa o Gerenciador do sistema ou a CLI do ONTAP.

Gestor do sistema - ONTAP 9.8 e posterior

1. Para exibir detalhes sobre uma licença de recurso específica, selecione **Cluster > Settings**.
2. Em **licenças**, selecione .
3. Selecione **recursos**.
4. Localize o recurso licenciado que deseja exibir e selecione para exibir os detalhes da licença.

Gestor do sistema - ONTAP 9.7 e anteriores

1. Selecione **Configuração > Cluster > licenças**.
2. Na janela **Licenses**, execute a ação apropriada:
3. Clique na guia **Detalhes**.

CLI

1. Exibir detalhes sobre uma licença instalada:

```
system license show
```

Eliminar uma licença

Gestor do sistema - ONTAP 9.8 e posterior

1. Para eliminar uma licença, selecione **Cluster > Settings**.
2. Em **licenças**, selecione .
3. Selecione **recursos**.
4. Selecione o recurso licenciado que deseja excluir e **Excluir chave legada**.

Gestor do sistema - ONTAP 9.7 e anteriores

1. Selecione **Configuração > Cluster > licenças**.
2. Na janela **Licenses**, execute a ação apropriada:

Se você quiser…	Faça isso…
Exclua um pacote de licença específico em um nó ou uma licença mestre	Clique na guia **Detalhes**.
Exclua um pacote de licença específico em todos os nós do cluster	Clique na guia **Pacotes**.

3. Selecione o pacote de licença de software que deseja excluir e clique em **Excluir**.

   Você pode excluir apenas um pacote de licença de cada vez.

4. Marque a caixa de seleção de confirmação e clique em **Excluir**.

CLI

1. Eliminar uma licença:

   ```
   system license delete
   ```

   O exemplo a seguir exclui uma licença chamada CIFS e o número de série 1-81-0000000000000000000123456 do cluster:

   ```
   cluster1::> system license delete -serial-number 1-81-
   0000000000000000000123456 -package CIFS
   ```

   O exemplo a seguir exclui do cluster todas as licenças sob o pacote núcleo da licença instalada para o número de série 123456789:

   ```
   cluster1::> system license delete { -serial-number 123456789
   -installed-license "Core Bundle" }
   ```

Informações relacionadas

"Comandos CLI do ONTAP para gerenciar licenças"

"Referência do comando ONTAP"

Tipos de licença e método licenciado

A compreensão dos tipos de licença e do método licenciado ajuda a gerenciar as licenças em um cluster.

Tipos de licença

Um pacote pode ter um ou mais dos seguintes tipos de licença instalados no cluster. O `system license show` comando exibe o tipo ou tipos de licença instalados para um pacote.

- Licença (`license`padrão)

  Uma licença padrão é uma licença de nó bloqueado. Ele é emitido para um nó com um número de série específico do sistema (também conhecido como *número de série do controlador*). Uma licença padrão é válida apenas para o nó que tem o número de série correspondente.

  A instalação de uma licença padrão de bloqueio de nó dá direito a um nó à funcionalidade licenciada. Para que o cluster use a funcionalidade licenciada, pelo menos um nó deve ser licenciado para a funcionalidade. Pode estar fora de conformidade usar a funcionalidade licenciada em um nó que não tenha direito à funcionalidade.

- Licença local (`site`)

  Uma licença de local não está vinculada a um número de série específico do sistema. Quando você instala uma licença de site, todos os nós no cluster têm direito à funcionalidade licenciada. O `system license show` comando exibe as licenças do site sob o número de série do cluster.

  Se o cluster tiver uma licença de site e você remover um nó do cluster, o nó não carregará a licença de site com ele e não terá mais direito à funcionalidade licenciada. Se você adicionar um nó a um cluster que tenha uma licença de site, o nó terá automaticamente direito à funcionalidade concedida pela licença de site.

- Licença de avaliação (`demo`)

  Uma licença de avaliação é uma licença temporária que expira após um determinado período de tempo (indicado pelo `system license show` comando). Ele permite que você experimente determinadas funcionalidades de software sem comprar um direito. É uma licença em todo o cluster e não está vinculada a um número de série específico de um nó.

  Se o cluster tiver uma licença de avaliação para um pacote e você remover um nó do cluster, o nó não carregará a licença de avaliação com ele.

Método licenciado

É possível instalar uma licença em todo o cluster (o `site` tipo ou `demo`) e uma licença de nó bloqueado (o `license` tipo) para um pacote. Portanto, um pacote instalado pode ter vários tipos de licença no cluster. No entanto, para o cluster, há apenas um método *licenciado* para um pacote. O `licensed method` campo `system license status show` do comando exibe o direito que está sendo usado para um pacote. O comando determina o método licenciado da seguinte forma:

- Se um pacote tiver apenas um tipo de licença instalado no cluster, o tipo de licença instalada é o método

licenciado.

- Se um pacote não tiver nenhuma licença instalada no cluster, o método licenciado será `none`.
- Se um pacote tiver vários tipos de licença instalados no cluster, o método licenciado será determinado na seguinte ordem de prioridade do tipo de licença--`site`, `license` e `demo`.

  Por exemplo:

  - Se você tiver uma licença de site, uma licença padrão e uma licença de avaliação para um pacote, o método licenciado para o pacote no cluster é `site`.
  - Se você tiver uma licença padrão e uma licença de avaliação para um pacote, o método licenciado para o pacote no cluster é `license`.
  - Se você tiver apenas uma licença de avaliação para um pacote, o método licenciado para o pacote no cluster é `demo`.

Comandos para gerenciar licenças no ONTAP

Você pode usar os comandos da CLI do ONTAP `system license` para gerenciar licenças de recursos para o cluster. Você usa os `system feature-usage` comandos para monitorar o uso de recursos.

Saiba mais sobre os comandos descritos neste tópico no "Referência do comando ONTAP".

A tabela a seguir lista alguns dos comandos CLI comuns para gerenciar licenças e links para as páginas de manual do comando para obter informações adicionais.

Se você quiser…	Use este comando…
Exiba todos os pacotes que exigem licenças e seu status de licença atual, incluindo o seguinte: • O nome do pacote • O método licenciado • A data de validade, se aplicável	"show-status da licença do sistema"
Exibir ou remover licenças expiradas ou não utilizadas	"limpeza da licença do sistema"
Exiba o resumo do uso de recursos no cluster por nó	"show-resumo do uso de recursos do sistema"
Exiba o status de uso do recurso no cluster por nó e por semana	"histórico de exibição de uso de recursos do sistema"
Exibir o status do risco de direito de licença para cada pacote de licença	"show de risco de direitos de licença do sistema"

Informações relacionadas

- "Referência do comando ONTAP"
- "artigo da base de conhecimento: ONTAP 9.10,1 e visão geral do licenciamento posterior"
- "Use o Gerenciador do sistema para instalar um arquivo de licença do NetApp"

Gerenciamento de clusters com a CLI

Visão geral da administração com a CLI

Você pode administrar sistemas ONTAP com a interface de linha de comando (CLI). Você pode usar as interfaces de gerenciamento do ONTAP, acessar o cluster, gerenciar nós e muito mais.

Você deve usar esses procedimentos nas seguintes circunstâncias:

- Você quer entender a gama de recursos de administrador do ONTAP.
- Você deseja usar a CLI, não o System Manager ou uma ferramenta de script automatizado.

Informações relacionadas

Para obter detalhes sobre a sintaxe e o uso da CLI, consulte "Referência do comando ONTAP"a documentação.

Administradores de clusters e SVM

Administradores de clusters e SVM

Os administradores de cluster administram todo o cluster e as máquinas virtuais de armazenamento (SVMs, anteriormente conhecidas como VServers) que ele contém. Os administradores do SVM administram apenas seus próprios SVMs de dados.

Os administradores de cluster podem administrar todo o cluster e seus recursos. Eles também podem configurar SVMs de dados e delegar a administração da SVM aos administradores do SVM. Os recursos específicos que os administradores de cluster têm dependem de suas funções de controle de acesso. Por padrão, um administrador de cluster com o nome de conta "'admin'" ou nome de função tem todos os recursos para gerenciar o cluster e SVMs.

Os administradores do SVM podem administrar apenas seus próprios recursos de rede e storage SVM, como volumes, protocolos, LIFs e serviços. As funcionalidades específicas que os administradores do SVM têm dependem das funções de controle de acesso atribuídas pelos administradores de cluster.

A interface de linha de comando (CLI) do ONTAP continua a usar o termo *SVM* na saída, e `vserver` como um nome de comando ou parâmetro não foi alterado.

Gerencie o acesso ao System Manager

Você pode ativar ou desativar o acesso de um navegador da Web ao System Manager. Você também pode visualizar o log do System Manager.

Você pode controlar o acesso de um navegador da Web ao System Manager usando `vserver services`

`web modify -name sysmgr -vserver` *`cluster_name`* `-enabled [true|false]`.

O log do System Manager é gravado `/mroot/etc/log/mlog/sysmgr.log` nos arquivos do nó que hospeda o LIF de gerenciamento de cluster no momento em que o System Manager é acessado. Você pode visualizar os arquivos de log usando um navegador. O log do Gerenciador de sistema também está incluído nas mensagens do AutoSupport.

O que é o servidor de gerenciamento de cluster

O servidor de gerenciamento de cluster, também chamado de *admin*SVM, é uma implementação especializada de máquina virtual de storage (SVM) que apresenta o cluster como uma única entidade gerenciável. Além de servir como o domínio administrativo de mais alto nível, o servidor de gerenciamento de clusters possui recursos que não pertencem logicamente a um SVM de dados.

O servidor de gerenciamento de cluster está sempre disponível no cluster. Você pode acessar o servidor de gerenciamento de cluster por meio do console ou do LIF de gerenciamento de cluster.

Após a falha de sua porta de rede doméstica, o LIF de gerenciamento de cluster automaticamente faz failover para outro nó no cluster. Dependendo das caraterísticas de conetividade do protocolo de gerenciamento que você está usando, você pode ou não notar o failover. Se você estiver usando um protocolo sem conexão (por exemplo, SNMP) ou tiver uma conexão limitada (por exemplo, HTTP), é provável que você não perceba o failover. No entanto, se você estiver usando uma conexão de longo prazo (por exemplo, SSH), então você terá que se reconetar ao servidor de gerenciamento de cluster após o failover.

Quando você cria um cluster, todas as caraterísticas do LIF de gerenciamento de cluster são configuradas, incluindo seu endereço IP, máscara de rede, gateway e porta.

Diferentemente de um SVM ou nó de dados, um servidor de gerenciamento de cluster não tem volume raiz ou volumes de usuário de host (embora possa hospedar volumes do sistema). Além disso, um servidor de gerenciamento de cluster só pode ter LIFs do tipo de gerenciamento de cluster.

Se você executar o `vserver show` comando, o servidor de gerenciamento de cluster aparecerá na lista de saída para esse comando.

Tipos de SVMs

Um cluster consiste em quatro tipos de SVMs, que ajudam a gerenciar o cluster e seus recursos e acesso a dados aos clientes e aplicações.

Um cluster contém os seguintes tipos de SVMs:

- SVM admin

  O processo de configuração do cluster cria automaticamente o administrador SVM para o cluster. O SVM admin representa o cluster.

- SVM de nó

  Um nó SVM é criado quando o nó se junta ao cluster e o nó SVM representa os nós individuais do cluster.

- SVM do sistema (avançado)

Um SVM do sistema é criado automaticamente para comunicações no nível do cluster em um espaço IPspace.

- Data SVM

  Um data SVM representa os dados que atendem SVMs. Após a configuração do cluster, um administrador de cluster deve criar SVMs de dados e adicionar volumes a essas SVMs para facilitar o acesso aos dados a partir do cluster.

  Um cluster precisa ter pelo menos um SVM de dados para servir dados a seus clientes.

> Salvo especificação em contrário, o termo SVM se refere a um SVM de dados (fornecimento de dados).
>
> Na CLI, os SVMs são exibidos como VServers.

Acessar o cluster usando a CLI (somente administradores de cluster)

Acesse o cluster usando a porta serial

Você pode acessar o cluster diretamente de um console conetado à porta serial de um nó.

Passos

1. No console, pressione Enter.

   O sistema responde com o aviso de início de sessão.

2. No prompt de login, execute um dos seguintes procedimentos:

Para acessar o cluster com…	Digite o seguinte nome de conta…
A conta de cluster predefinida	**`admin`**
Uma conta de usuário administrativa alternativa	*`username`*

   O sistema responde com o aviso de palavra-passe.

3. Introduza a palavra-passe da conta de utilizador administrativo ou administrativo e, em seguida, prima Enter.

Acesse o cluster usando SSH

Você pode emitir solicitações SSH para um cluster ONTAP para executar tarefas administrativas. O SSH está ativado por predefinição.

Antes de começar

- Você deve ter uma conta de usuário configurada para usar `ssh` como método de acesso.

  O `-application` parâmetro dos[`security login` comandos especifica o método de acesso para uma conta de usuário. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-

login-create.html[`security login` na referência de comando do ONTAP.

- Se você usar uma conta de usuário de domínio do ative Directory (AD) para acessar o cluster, um túnel de autenticação para o cluster deve ter sido configurado por meio de uma VM de armazenamento habilitada para CIFS e sua conta de usuário de domínio do AD também deve ter sido adicionada ao cluster `ssh` como método de acesso e `domain` como método de autenticação.

Sobre esta tarefa

- Você deve usar um cliente OpenSSH 5,7 ou posterior.
- Apenas o protocolo SSH v2 é suportado; o SSH v1 não é suportado.
- O ONTAP suporta um máximo de 64 sessões de SSH simultâneas por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de conexões de entrada for superior a 10 por segundo, o serviço será temporariamente desativado por 60 segundos.

- O ONTAP suporta apenas os algoritmos de criptografia AES e 3DES (também conhecidos como *cifras*) para SSH.

  O AES é suportado com 128, 192 e 256 bits no comprimento da chave. 3DES tem 56 bits no comprimento da chave como no DES original, mas é repetido três vezes.

- Quando o modo FIPS está ativado, os clientes SSH devem negociar com algoritmos de chave pública Elliptic Curve Digital Signature Algorithm (ECDSA) para que a conexão seja bem-sucedida.
- Se você quiser acessar a CLI do ONTAP a partir de um host do Windows, você pode usar um utilitário de terceiros, como o PuTTY.
- Se você usar um nome de usuário do Windows AD para fazer login no ONTAP, use as mesmas letras maiúsculas ou minúsculas que foram usadas quando o nome de usuário e o nome de domínio do AD foram criados no ONTAP.

  Os nomes de usuários DE ANÚNCIOS e nomes de domínio não diferenciam maiúsculas de minúsculas. No entanto, os nomes de usuário do ONTAP são sensíveis a maiúsculas e minúsculas. A incompatibilidade de casos entre o nome de utilizador criado no ONTAP e o nome de utilizador criado no AD resulta numa falha de início de sessão.

Opções de autenticação SSH

- A partir do ONTAP 9.3, você pode "Ative a autenticação multifator SSH" para contas de administrador locais.

  Quando a autenticação multifator SSH está ativada, os usuários são autenticados usando uma chave pública e uma senha.

- A partir do ONTAP 9.4, você pode "Ative a autenticação multifator SSH" para usuários remotos LDAP e NIS.
- A partir do ONTAP 9.13,1, você pode opcionalmente adicionar validação de certificado ao processo de autenticação SSH para melhorar a segurança de login. Para fazer isso, "Associar um certificado X,509 à chave pública"uma conta usa. Se você fizer login usando SSH com uma chave pública SSH e um certificado X,509, o ONTAP verificará a validade do certificado X,509 antes de autenticar com a chave pública SSH. O login SSH é recusado se esse certificado estiver expirado ou revogado e a chave pública SSH for desativada automaticamente.

- A partir do ONTAP 9.14,1, os administradores do ONTAP podem "Adicione a autenticação de dois fatores do Cisco Duo ao processo de autenticação SSH"melhorar a segurança de login. Após o primeiro login depois de ativar a autenticação Cisco Duo, os usuários precisarão Registrar um dispositivo para servir como autenticador para sessões SSH.
- A partir do ONTAP 9.15,1, os administradores podem "Configurar autorização dinâmica"fornecer autenticação adaptativa adicional aos usuários SSH com base na pontuação de confiança do usuário.

Passos

1. A partir de um host com acesso à rede do cluster ONTAP, digite o `ssh` comando em um dos seguintes formatos:
   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

Se você estiver usando uma conta de usuário de domínio do AD, você deve especificar *username* no formato *domainname**AD_accountname* (com backslashes duplos após o nome de domínio) ou "*domainname**AD_accountname*" (entre aspas duplas e com uma única barra invertida após o nome de domínio).

hostname_or_IP É o nome do host ou o endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nós. Recomenda-se a utilização do LIF de gestão de clusters. Você pode usar um endereço IPv4 ou IPv6.

command Não é necessário para sessões interativas SSH.

Exemplos de solicitações SSH

Os exemplos a seguir mostram como a conta de usuário chamada "joe" pode emitir uma solicitação SSH para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Os exemplos a seguir mostram como a conta de usuário chamada "john" do domínio chamado "domain1"

pode emitir uma solicitação SSH para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

O exemplo a seguir mostra como a conta de usuário chamada "joe" pode emitir uma solicitação SSH MFA para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Informações relacionadas

"Autenticação de administrador e RBAC"

Segurança de login SSH

A partir do ONTAP 9.5, você pode exibir informações sobre logins anteriores, tentativas malsucedidas de fazer login e alterações no Privileges desde o último login bem-sucedido.

As informações relacionadas à segurança são exibidas quando você faz login com sucesso como um usuário de administrador SSH. Você é alertado sobre as seguintes condições:

- A última vez que o nome da sua conta foi iniciado.
- O número de tentativas de login mal sucedidas desde o último login bem-sucedido.
- Se a função mudou desde o último login (por exemplo, se a função da conta de administrador mudou de "admin" para "backup".)
- Se os recursos de adição, modificação ou exclusão da função foram modificados desde o último login.

> Se alguma das informações apresentadas for suspeita, deverá contactar imediatamente o seu departamento de segurança.

Para obter essas informações quando você fizer login, os seguintes pré-requisitos devem ser atendidos:

- Sua conta de usuário SSH deve ser provisionada no ONTAP.
- Seu login de segurança SSH deve ser criado.
- Sua tentativa de login deve ser bem-sucedida.

Restrições e outras considerações para segurança de login SSH

As seguintes restrições e considerações se aplicam às informações de segurança de login SSH:

- As informações estão disponíveis apenas para logins baseados em SSH.
- Para contas de administrador baseadas em grupo, como contas LDAP/NIS e AD, os usuários podem exibir as informações de login SSH se o grupo do qual são membros for provisionado como uma conta de administrador no ONTAP.

  No entanto, alertas sobre alterações na função da conta de usuário não podem ser exibidos para esses usuários. Além disso, os usuários pertencentes a um grupo AD que tenha sido provisionado como uma conta de administrador no ONTAP não podem exibir a contagem de tentativas de login mal sucedidas que ocorreram desde a última vez em que fizeram login.
- As informações mantidas para um usuário são excluídas quando a conta de usuário é excluída do ONTAP.
- As informações não são exibidas para conexões a aplicativos que não sejam SSH.

Exemplos de informações de segurança de login SSH

Os exemplos a seguir demonstram o tipo de informação exibida após o login.

- Esta mensagem é apresentada após cada início de sessão bem-sucedido:

```
Last Login : 7/19/2018 06:11:32
```

- Estas mensagens são apresentadas se não tiverem sido efetuadas tentativas de início de sessão sem êxito desde o último início de sessão bem-sucedido:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Estas mensagens são apresentadas se não tiverem sido efetuadas tentativas de início de sessão sem êxito e o seu Privileges tiver sido modificado desde o último início de sessão bem-sucedido:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Ative o acesso Telnet ou RSH ao cluster

Como prática recomendada de segurança, Telnet e RSH são desativados por padrão. Para permitir que o cluster aceite solicitações Telnet ou RSH, você deve ativar o serviço na política de serviço de gerenciamento padrão.

Telnet e RSH não são protocolos seguros; você deve considerar o uso de SSH para acessar o cluster. O SSH fornece um shell remoto seguro e sessão de rede interativa. Para obter mais informações, "Acesse o cluster usando SSH"consulte .

Sobre esta tarefa

- O ONTAP suporta um máximo de 50 sessões simultâneas de Telnet ou RSH por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de conexões de entrada for superior a 10 por segundo, o serviço será temporariamente desativado por 60 segundos.

- Os comandos RSH requerem Privileges avançado.

ONTAP 9.10,1 ou posterior

Passos

1. Confirme se o protocolo de segurança RSH ou Telnet está ativado:

   ```
   security protocol show
   ```

   a. Se o protocolo de segurança RSH ou Telnet estiver ativado, avance para o passo seguinte.

   b. Se o protocolo de segurança RSH ou Telnet não estiver ativado, use o seguinte comando para ativá-lo:

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

2. Confirme se o `management-rsh-server` serviço ou `management-telnet-server` existe nas LIFs de gerenciamento:

   ```
   network interface show -services management-rsh-server
   ```

   ou

   ```
   network interface show -services management-telnet-server
   ```

   a. Se o `management-rsh-server` serviço ou `management-telnet-server` existir, avance para o passo seguinte.

   b. Se o `management-rsh-server` serviço ou `management-telnet-server` não existir, use o seguinte comando para adicioná-lo:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   ```
   network interface service-policy add-service -vserver cluster1 -policy
   default-management -service management-telnet-server
   ```

ONTAP 9 1.9 ou anterior

Sobre esta tarefa

O ONTAP impede que você altere políticas de firewall predefinidas, mas você pode criar uma nova política clonando a política de firewall de gerenciamento predefinida `mgmt` e habilitando o Telnet ou o RSH sob a nova política.

Passos

1. Entre no modo de privilégio avançado:

   ```
   set advanced
   ```

2. Ativar um protocolo de segurança (RSH ou Telnet):

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. Crie uma nova política de firewall de gerenciamento com base na `mgmt` política de firewall de gerenciamento:

```
system services firewall policy clone -policy mgmt -destination-policy
policy-name
```

4. Ativar Telnet ou RSH na nova política de firewall de gerenciamento:

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   Para permitir todos os endereços IP, você deve especificar `-ip-list 0.0.0.0/0`

5. Associe a nova política ao LIF de gerenciamento de clusters:

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

Acesse o cluster usando Telnet

Você pode emitir solicitações Telnet para o cluster para executar tarefas administrativas. O Telnet está desativado por padrão.

Telnet e RSH não são protocolos seguros; você deve considerar o uso de SSH para acessar o cluster. O SSH fornece um shell remoto seguro e sessão de rede interativa. Para obter mais informações, "Acesse o cluster usando SSH"consulte .

Antes de começar

As condições a seguir devem ser atendidas antes que você possa usar o Telnet para acessar o cluster:

- Você deve ter uma conta de usuário local de cluster configurada para usar Telnet como método de acesso.

  O `-application` parâmetro dos `security login` comandos especifica o método de acesso para uma conta de usuário. Para obter mais informações, consulte as `security login` páginas de manual.

Sobre esta tarefa

- O ONTAP suporta um máximo de 50 sessões Telnet simultâneas por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de ligações em curso for superior a 10 por segundo, o serviço é temporariamente desativado durante 60 segundos.

- Se você quiser acessar a CLI do ONTAP a partir de um host do Windows, você pode usar um utilitário de terceiros, como o PuTTY.
- Os comandos RSH requerem Privileges avançado.

ONTAP 9.10,1 ou posterior

Passos

1. Confirme se o protocolo de segurança Telnet está ativado:

   `security protocol show`

   a. Se o protocolo de segurança Telnet estiver ativado, avance para o passo seguinte.

   b. Se o protocolo de segurança Telnet não estiver ativado, use o seguinte comando para ativá-lo:

      `security protocol modify -application telnet -enabled true`

2. Confirme se o `management-telnet-server` serviço existe nas LIFs de gerenciamento:

   `network interface show -services management-telnet-server`

   a. Se o `management-telnet-server` serviço existir, avance para o passo seguinte.

   b. Se o `management-telnet-server` serviço não existir, use o seguinte comando para adicioná-lo:

      `network interface service-policy add-service -vserver cluster1 -policy default-management -service management-telnet-server`

ONTAP 9 1.9 ou anterior

Antes de começar

As condições a seguir devem ser atendidas antes que você possa usar o Telnet para acessar o cluster:

- O Telnet já deve estar habilitado na política de firewall de gerenciamento usada pelas LIFs de gerenciamento de cluster ou nó para que as solicitações Telnet possam passar pelo firewall.

  Por padrão, o Telnet está desativado. O `system services firewall policy show` comando com o `-service telnet` parâmetro exibe se o Telnet foi habilitado em uma política de firewall. Para obter mais informações, consulte as `system services firewall policy` páginas de manual.

- Se você usar conexões IPv6, o IPv6 já deve estar configurado e habilitado no cluster e as políticas de firewall já devem ser configuradas com endereços IPv6.

  O `network options ipv6 show` comando exibe se o IPv6 está ativado. O `system services firewall policy show` comando exibe políticas de firewall.

Passos

1. Em um host de administração, digite o seguinte comando:

   `telnet hostname_or_IP`

   `hostname_or_IP` É o nome do host ou o endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nós. Recomenda-se a utilização do LIF de gestão de clusters. Você pode usar um endereço IPv4 ou IPv6.

Exemplo de uma solicitação Telnet

O exemplo a seguir mostra como o usuário chamado "joe", que foi configurado com acesso Telnet, pode emitir uma solicitação Telnet para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.28:

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Aceda ao cluster utilizando o RSH

Você pode emitir solicitações RSH ao cluster para executar tarefas administrativas. O RSH não é um protocolo seguro e está desativado por padrão.

Telnet e RSH não são protocolos seguros; você deve considerar o uso de SSH para acessar o cluster. O SSH fornece um shell remoto seguro e sessão de rede interativa. Para obter mais informações, "Acesse o cluster usando SSH"consulte .

Antes de começar

As seguintes condições devem ser cumpridas antes de poder utilizar o RSH para aceder ao cluster:

- Tem de ter uma conta de utilizador local de cluster configurada para utilizar o RSH como método de acesso.

  O `-application` parâmetro dos `security login` comandos especifica o método de acesso para uma conta de usuário. Para obter mais informações, consulte as `security login` páginas de manual.

Sobre esta tarefa

- O ONTAP suporta um máximo de 50 sessões de RSH simultâneas por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de conexões de entrada for superior a 10 por segundo, o serviço será temporariamente desativado por 60 segundos.

- Os comandos RSH requerem Privileges avançado.

ONTAP 9.10,1 ou posterior

Passos

1. Confirme se o protocolo de segurança RSH está ativado:

   `security protocol show`

   a. Se o protocolo de segurança RSH estiver ativado, avance para o passo seguinte.

   b. Se o protocolo de segurança RSH não estiver ativado, utilize o seguinte comando para o ativar:

      `security protocol modify -application rsh -enabled true`

2. Confirme se o `management-rsh-server` serviço existe nas LIFs de gerenciamento:

   `network interface show -services management-rsh-server`

   a. Se o `management-rsh-server` serviço existir, avance para o passo seguinte.

   b. Se o `management-rsh-server` serviço não existir, use o seguinte comando para adicioná-lo:

      `network interface service-policy add-service -vserver cluster1 -policy default-management -service management-rsh-server`

ONTAP 9 1.9 ou anterior

Antes de começar

As seguintes condições devem ser cumpridas antes de poder utilizar o RSH para aceder ao cluster:

- O RSH já deve estar habilitado na política de firewall de gerenciamento que é usada pelos LIFs de gerenciamento de cluster ou nó para que as solicitações RSH possam passar pelo firewall.

  Por predefinição, o RSH está desativado. O comando show de política de firewall de serviços do sistema com o `-service rsh` parâmetro exibe se o RSH foi ativado em uma política de firewall. Para obter mais informações, consulte as `system services firewall policy` páginas de manual.

- Se você usar conexões IPv6, o IPv6 já deve estar configurado e habilitado no cluster e as políticas de firewall já devem ser configuradas com endereços IPv6.

  O `network options ipv6 show` comando exibe se o IPv6 está ativado. O `system services firewall policy show` comando exibe políticas de firewall.

Passos

1. Em um host de administração, digite o seguinte comando:

   `rsh hostname_or_IP -l username:passwordcommand`

   `hostname_or_IP` É o nome do host ou o endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nós. Recomenda-se a utilização do LIF de gestão de clusters. Você pode usar um endereço IPv4 ou IPv6.

   `command` É o comando que você deseja executar sobre RSH.

Exemplo de uma solicitação RSH

O exemplo a seguir mostra como o usuário chamado "joe", que foi configurado com RSH Access, pode emitir uma solicitação RSH para executar o `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

Use a interface da linha de comando ONTAP

Usando a interface de linha de comando ONTAP

A interface de linha de comando (CLI) do ONTAP fornece uma visualização baseada em comando da interface de gerenciamento. Você insere comandos no prompt do sistema de armazenamento e os resultados do comando são exibidos no texto.

O prompt de comando CLI é representado como `cluster_name::>`.

Se você definir o nível de privilégio (ou seja, o `-privilege` parâmetro `set` do comando) como `advanced`, o prompt incluirá um asterisco (*), por exemplo:

```
cluster_name::*>
```

Sobre os diferentes shells para a visão geral dos comandos CLI (somente administradores de cluster)

O cluster tem três shells diferentes para comandos CLI, o *clustershell*, o *nodeshell* e o *systemshell*. Os shells são para finalidades diferentes, e cada um deles tem um conjunto de comandos diferente.

- O clustershell é o shell nativo que é iniciado automaticamente quando você faz login no cluster.

  Ele fornece todos os comandos que você precisa para configurar e gerenciar o cluster. A ajuda CLI do clustershell (acionada pelo `?` prompt do clustershell) exibe comandos disponíveis do clustershell. O `man *command_name*` comando no clustershell exibe a página de manual para o comando clustershell especificado.

- O nodeshell é um shell especial para comandos que entram em efeito apenas no nível do nó.

  O nodeshell é acessível através do `system node run` comando.

  A ajuda da CLI nodeshell (acionada por `?` ou `help` no prompt nodeshell) exibe os comandos nodeshell disponíveis. O `man *command_name*` comando no nodeshell exibe a página man para o comando nodeshell especificado.

Muitos comandos e opções de nodeshell comumente usados são tunneled ou aliased no clustershell e podem ser executados também a partir do clustershell.

- O systemshell é um shell de baixo nível que é usado apenas para fins de diagnóstico e solução de problemas.

  A estrutura do sistema e a conta "diag" associada destinam-se a fins de diagnóstico de baixo nível. Seu acesso requer o nível de privilégio de diagnóstico e é reservado apenas para o suporte técnico para executar tarefas de solução de problemas.

Acesso de comandos e opções nodeshell no clustershell

Os comandos e opções Nodeshell são acessíveis através do nodeshell:

`system node run –node` *`nodename`*

Muitos comandos e opções de nodeshell comumente usados são tunneled ou aliased no clustershell e podem ser executados também a partir do clustershell.

As opções Nodeshell que são suportadas no clustershell podem ser acessadas usando o `vserver options clustershell` comando. Para ver essas opções, você pode fazer um dos seguintes procedimentos:

- Consulte a CLI do clustershell com `vserver options -vserver` *`nodename_or_clustername`* `-option-name ?`
- Acesse a `vserver options` página man na CLI do clustershell com `man vserver options`

Se você inserir um comando nodeshell ou legacy ou opção no clustershell, e o comando ou opção tiver um comando conclustershell equivalente, o ONTAP informa você sobre o comando conclustershell a ser usado.

Se você inserir um comando nodeshell ou legacy ou uma opção que não é suportada no clustershell, o ONTAP informa o status "'não suportado'" para o comando ou opção.

Exibir comandos nodeshell disponíveis

Você pode obter uma lista de comandos nodeshell disponíveis usando a ajuda CLI do nodeshell.

Passos

1. Para acessar o nodeshell, digite o seguinte comando no prompt do sistema do clustershell:

   `system node run -node {`*`nodename`*`|local}`

   `local` é o nó usado para acessar o cluster.

   > O `system node run` comando tem um comando alias, `run`.

2. Digite o seguinte comando no nodeshell para ver a lista de comandos nodeshell disponíveis:

   `[`*`commandname`*`] help`

`_commandname_` é o nome do comando cuja disponibilidade você deseja exibir. Se você não incluir `_commandname_`, a CLI exibirá todos os comandos nodeshell disponíveis.

Você insere `exit` ou digita Ctrl-d para retornar à CLI do clustershell.

Exemplo de exibição de comandos nodeshell disponíveis

O exemplo a seguir acessa o nodeshell de um nó chamado node2 e exibe informações para o comando nodeshell `environment` :

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

Métodos de navegação de diretórios de comando CLI

Os comandos na CLI são organizados em uma hierarquia por diretórios de comando. Você pode executar comandos na hierarquia inserindo o caminho completo do comando ou navegando pela estrutura do diretório.

Ao usar a CLI, você pode acessar um diretório de comandos digitando o nome do diretório no prompt e pressionando Enter. O nome do diretório é então incluído no texto do prompt para indicar que você está interagindo com o diretório de comando apropriado. Para ir mais fundo para a hierarquia de comandos, digite o nome de um subdiretório de comandos seguido de pressionar Enter. O nome do subdiretório é então incluído no texto do prompt e o contexto muda para esse subdiretório.

Você pode navegar através de vários diretórios de comando inserindo o comando inteiro. Por exemplo, você pode exibir informações sobre unidades de disco digitando o `storage disk show` comando no prompt. Você também pode executar o comando navegando por um diretório de comando de cada vez, como mostrado no exemplo a seguir:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Você pode abreviar comandos inserindo apenas o número mínimo de letras em um comando que torna o comando exclusivo para o diretório atual. Por exemplo, para abreviar o comando no exemplo anterior, você

pode digitar `st d sh`. Você também pode usar a tecla Tab para expandir comandos abreviados e exibir os parâmetros de um comando, incluindo valores de parâmetro padrão.

Você pode usar o `top` comando para ir para o nível superior da hierarquia de comandos e o `up` comando ou `..` comando para subir um nível na hierarquia de comandos.

Comandos e opções de comando precedidos por um asterisco (*) na CLI só podem ser executados no nível de privilégio avançado ou superior.

Regras para especificar valores na CLI

A maioria dos comandos inclui um ou mais parâmetros necessários ou opcionais. Muitos parâmetros exigem que você especifique um valor para eles. Existem algumas regras para especificar valores na CLI.

- Um valor pode ser um número, um especificador booleano, uma seleção de uma lista enumerada de valores predefinidos ou uma cadeia de texto.

  Alguns parâmetros podem aceitar uma lista separada por vírgulas de dois ou mais valores. Listas de valores separados por vírgulas não precisam estar entre aspas (" "). Sempre que você especificar texto, um espaço ou um caractere de consulta (quando não se entende como uma consulta ou texto começando com um símbolo menor ou maior), você deve incluir a entidade entre aspas.

- A CLI interpreta um ponto de interrogação ("?"") como o comando para exibir informações de ajuda para um determinado comando.
- Algum texto inserido na CLI, como nomes de comandos, parâmetros e determinados valores, não diferencia maiúsculas de minúsculas.

  Por exemplo, quando você insere valores de parâmetro para os `vserver cifs` comandos, a capitalização é ignorada. No entanto, a maioria dos valores de parâmetros, como os nomes de nós, máquinas virtuais de storage (SVMs), agregados, volumes e interfaces lógicas, são sensíveis a maiúsculas e minúsculas.

- Se você quiser limpar o valor de um parâmetro que recebe uma string ou uma lista, especifique um conjunto vazio de aspas ("") ou um traço ("-").
- O sinal de hash (""#""), também conhecido como sinal de libra, indica um comentário para uma entrada de linha de comando; se usado, ele deve aparecer após o último parâmetro em uma linha de comando.

  A CLI ignora o texto entre o número "" e o fim da linha.

No exemplo a seguir, um SVM é criado com um comentário de texto. O SVM é então modificado para excluir o comentário:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

No exemplo a seguir, um comentário de linha de comando que usa o sinal de "#" indica o que o comando faz.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Métodos de visualização do histórico de comandos e reemissão de comandos

Cada sessão CLI mantém um histórico de todos os comandos emitidos nela. Você pode ver o histórico de comandos da sessão em que está atualmente. Você também pode reemitir comandos.

Para visualizar o histórico de comandos, pode utilizar o `history` comando.

Para reemitir um comando, você pode usar o `redo` comando com um dos seguintes argumentos:

- Uma cadeia de carateres que corresponde a parte de um comando anterior

  Por exemplo, se o único `volume` comando executado for `volume show`, você poderá usar o `redo volume` comando para reexecutar o comando.

- O ID numérico de um comando anterior, conforme listado pelo `history` comando

  Por exemplo, você pode usar o `redo 4` comando para reemitir o quarto comando na lista de histórico.

- Um desvio negativo a partir do final da lista de histórico

  Por exemplo, você pode usar o `redo -2` comando para reemitir o comando que você executou dois comandos atrás.

Por exemplo, para refazer o comando que está em terceiro lugar do final do histórico de comandos, digite o seguinte comando:

```
cluster1::> redo -3
```

Atalhos de teclado para editar comandos CLI

O comando no prompt de comando atual é o comando ativo. O uso de atalhos de teclado permite que você edite o comando ativo rapidamente. Esses atalhos de teclado são semelhantes aos do shell UNIX tcsh e do editor Emacs.

A tabela a seguir lista os atalhos de teclado para editar comandos CLI. ""Ctrl-"" indica que você pressiona e mantém pressionada a tecla Ctrl enquanto digita o caractere especificado após ele. "'Esc-" indica que você pressiona e solta a tecla ESC e, em seguida, digita o caractere especificado após ela.

Se você quiser…	Use o seguinte atalho de teclado…
Mova o cursor para trás por um caractere	Ctrl-B

Se você quiser…	Use o seguinte atalho de teclado…
Seta para trás	Mova o cursor para a frente por um caractere
Ctrl-F	Seta para a frente
Mova o cursor para trás por uma palavra	ESC-B
Mova o cursor para a frente por uma palavra	ESC-F
Mova o cursor para o início da linha	Ctrl-A
Mova o cursor para o fim da linha	Ctrl-e
Remova o conteúdo da linha de comando do início da linha para o cursor e salve-o no buffer de corte. O buffer de corte age como memória temporária, semelhante ao que é chamado de *clipboard* em alguns programas.	Ctrl-U
Remova o conteúdo da linha de comando do cursor até o final da linha e salve-o no buffer de corte	Ctrl-K
Remova o conteúdo da linha de comando do cursor até o final da palavra a seguir e salve-o no buffer de corte	ESC-D
Remova a palavra antes do cursor e salve-a no buffer de corte	Ctrl-W
Yank o conteúdo do buffer de corte, e empurre-o para a linha de comando no cursor	Ctrl-Y
Exclua o caractere antes do cursor	Ctrl-H
Backspace	Exclua o caractere onde o cursor está
Ctrl-D	Limpe a linha
Ctrl-C	Limpe o ecrã
Ctrl-L	Substitua o conteúdo atual da linha de comando pela entrada anterior na lista de histórico. Com cada repetição do atalho de teclado, o cursor do histórico move-se para a entrada anterior.

Se você quiser…	Use o seguinte atalho de teclado…
Ctrl-P	ESC-P
Seta para cima	Substitua o conteúdo atual da linha de comando pela próxima entrada na lista de histórico. Com cada repetição do atalho de teclado, o cursor do histórico move-se para a próxima entrada.
Ctrl-N	ESC-N
Seta para baixo	Expanda um comando parcialmente inserido ou liste entrada válida da posição de edição atual
Separador	Ctrl-I
Exibir ajuda sensível ao contexto	?
Escapar do mapeamento especial para o ponto de interrogação (" ?'?`") character. For instance, to enter a question mark into a command's argument, press Esc and then the "`" caractere.	ESC-?
Iniciar saída TTY	Ctrl-Q
Parar a saída TTY	Ctrl-S

Utilização de níveis de privilégios administrativos

Os comandos e parâmetros do ONTAP são definidos em três níveis de privilégio: *Admin*, *Advanced* e *diagnostic*. Os níveis de privilégio refletem os níveis de habilidade necessários na execução das tarefas.

- **admin**

  A maioria dos comandos e parâmetros estão disponíveis neste nível. Eles são usados para tarefas comuns ou rotineiras.

- **avançado**

  Comandos e parâmetros neste nível são usados com pouca frequência, exigem conhecimentos avançados e podem causar problemas se usados de forma inadequada.

  Você usa comandos ou parâmetros avançados apenas com o Conselho do pessoal de suporte.

- **diagnóstico**

  Comandos e parâmetros de diagnóstico são potencialmente disruptivos. Eles são usados apenas pelo pessoal de suporte para diagnosticar e corrigir problemas.

Defina o nível de privilégio na CLI

Você pode definir o nível de privilégio na CLI usando o `set` comando. As alterações nas configurações de nível de privilégio aplicam-se apenas à sessão em que você está. Elas não são persistentes em todas as sessões.

Passos

1. Para definir o nível de privilégio na CLI, use o `set` comando com o `-privilege` parâmetro.

Exemplo de definição do nível de privilégio

O exemplo a seguir define o nível de privilégio como avançado e depois como admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

Defina as preferências de exibição na CLI

Você pode definir preferências de exibição para uma sessão CLI usando o `set` comando e `rows` o comando. As preferências definidas aplicam-se apenas à sessão em que se encontra. Elas não são persistentes em todas as sessões.

Sobre esta tarefa

Você pode definir as seguintes preferências de exibição da CLI:

- O nível de privilégio da sessão de comando
- Se as confirmações são emitidas para comandos potencialmente disruptivos
- Se `show` os comandos exibem todos os campos
- O caractere ou carateres a serem usados como separador de campo
- A unidade padrão ao relatar tamanhos de dados
- O número de linhas que a tela exibe na sessão atual da CLI antes que a interface interrompa a saída

  Se o número preferido de linhas não for especificado, ele será ajustado automaticamente com base na altura real do terminal. Se a altura real for indefinida, o número padrão de linhas é 24.

- O nó ou a máquina virtual de storage padrão (SVM)
- Se um comando contínuo deve parar se encontrar um erro

Passos

1. Para definir preferências de exibição da CLI, use o `set` comando.

   Para definir o número de linhas que a tela exibe na sessão atual da CLI, você também pode usar o `rows` comando.

Para obter mais informações, consulte as páginas man para o `set` comando e `rows` comando.

Exemplo de configuração de preferências de exibição na CLI

O exemplo a seguir define uma vírgula para ser o separador de campos, define `GB` como a unidade padrão de tamanho de dados e define o número de linhas como 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Métodos de uso de operadores de consulta

A interface de gerenciamento suporta consultas e padrões de estilo UNIX e wildcards para permitir que você combine vários valores em argumentos de comando-parâmetro.

A tabela a seguir descreve os operadores de consulta suportados:

Operador	Descrição
*	Curinga que corresponde a todas as entradas. Por exemplo, o comando `volume show -volume *tmp*` exibe uma lista de todos os volumes cujos nomes incluem a cadeia de carateres `tmp`.
!	NÃO operador. Indica um valor que não deve ser correspondido; por exemplo, **`!vs0`** indica não corresponder ao valor `vs0`.
OU operador. Separa dois valores que devem ser comparados; por exemplo, `*vs0	vs2*` corresponde a vs0 ou VS2. Você pode especificar várias INSTRUÇÕES OU; por exemplo, `a
b*	*c*` corresponde à entrada `a`, qualquer entrada que comece com `b`, e qualquer entrada que inclua `c`.

Operador	Descrição
..	Operador de gama. Por exemplo, **`5..10`** corresponde a qualquer valor de `5` a `10`, inclusive.
*	Menos do que o operador. Por exemplo, **`<20`** corresponde a qualquer valor inferior `20` a .
>	Operador superior a. Por exemplo, **`>5`** corresponde a qualquer valor maior que `5`.
O que é que é	Menos ou igual ao operador. Por exemplo, ⇐**`5`** corresponde a qualquer valor menor ou igual a `5`.
>	Maior ou igual ao operador. Por exemplo, **`>=5`** corresponde a qualquer valor maior ou igual a `5`.
{`query`Selecione	Consulta alargada. Uma consulta estendida deve ser especificada como o primeiro argumento após o nome do comando, antes de quaisquer outros parâmetros. Por exemplo, o comando `volume modify {-volume *tmp*} -state offline` define offline todos os volumes cujos nomes incluem a cadeia de carateres `tmp`.

Se você quiser analisar carateres de consulta como literais, você deve incluir os carateres em aspas duplas (por exemplo, `"<10"` `"0..100"` , , `"*abc*"` ou `"a|b"`) para que os resultados corretos sejam retornados.

Você deve incluir nomes de arquivos brutos em aspas duplas para evitar a interpretação de carateres especiais. Isso também se aplica a carateres especiais usados pelo clustershell.

Você pode usar vários operadores de consulta em uma linha de comando. Por exemplo, o comando `volume show -size >1GB -percent-used <50 -vserver !vs1` exibe todos os volumes com mais de 1 GB de tamanho, menos de 50% utilizados e não na máquina virtual de armazenamento (SVM) chamada "'VS1".

Informações relacionadas

"Atalhos de teclado para editar comandos CLI"

Métodos de uso de consultas estendidas

Você pode usar consultas estendidas para corresponder e executar operações em objetos que tenham valores especificados.

Você especifica consultas estendidas, anexando-as entre colchetes encaracolados ("colchetes"). Uma

consulta estendida deve ser especificada como o primeiro argumento após o nome do comando, antes de quaisquer outros parâmetros. Por exemplo, para definir offline todos os volumes cujos nomes incluem a cadeia de carateres `tmp`, execute o comando no exemplo a seguir:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Consultas estendidas geralmente são úteis apenas com `modify` comandos e `delete`. Eles não têm nenhum significado em `create` ou `show` comandos.

A combinação de consultas e operações de modificação é uma ferramenta útil. No entanto, ele pode potencialmente causar confusão e erros se implementado incorretamente. Por exemplo, usar o comando (privilégio avançado) `system node image modify` para definir a imagem de software padrão de um nó automaticamente define a outra imagem de software para não ser a padrão. O comando no exemplo a seguir é efetivamente uma operação nula:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Este comando define a imagem padrão atual como a imagem não padrão e, em seguida, define a nova imagem padrão (a imagem não padrão anterior) para a imagem não padrão, resultando na retenção das configurações padrão originais. Para executar a operação corretamente, você pode usar o comando como indicado no exemplo a seguir:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Métodos de personalização da saída do comando show usando campos

Quando você usa o `-instance` parâmetro com um `show` comando para exibir detalhes, a saída pode ser longa e incluir mais informações do que você precisa. O `-fields` parâmetro de um `show` comando permite exibir apenas as informações especificadas.

Por exemplo, é provável que a execução `volume show -instance` resulte em várias telas de informações. Você pode usar `volume show -fields` *`fieldname[,fieldname…]`* para personalizar a saída de modo que ela inclua apenas o campo ou campos especificados (além dos campos padrão que são sempre exibidos). Você pode usar `-fields ?` para exibir campos válidos para um `show` comando.

O exemplo a seguir mostra a diferença de saída entre o `-instance` parâmetro e o `-fields` parâmetro:

```
cluster1::> volume show -instance

                                  Vserver Name: cluster1-1
                                   Volume Name: vol0
                                Aggregate Name: aggr0
                                   Volume Size: 348.3GB
                            Volume Data Set ID: -
                     Volume Master Data Set ID: -
                                  Volume State: online
                                   Volume Type: RW
                                  Volume Style: flex
                                           ...
                        Space Guarantee Style: volume
                     Space Guarantee in Effect: true
                                           ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- ----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

Sobre parâmetros posicionais

Você pode aproveitar a funcionalidade de parâmetro posicional da CLI do ONTAP para aumentar a eficiência na entrada de comandos. Você pode consultar um comando para identificar parâmetros que são posicionais para o comando.

O que é um parâmetro posicional

- Um parâmetro posicional é um parâmetro que não requer que você especifique o nome do parâmetro antes de especificar o valor do parâmetro.
- Um parâmetro posicional pode ser intercalado com parâmetros não posicionais na entrada do comando, desde que observe sua sequência relativa com outros parâmetros posicionais no mesmo comando, como

indicado na ***command_name ?*** saída.

- Um parâmetro posicional pode ser um parâmetro obrigatório ou opcional para um comando.
- Um parâmetro pode ser posicional para um comando, mas não posicional para outro.

> O uso da funcionalidade de parâmetro posicional em scripts não é recomendado, especialmente quando os parâmetros posicionais são opcionais para o comando ou têm parâmetros opcionais listados antes deles.

Identificar um parâmetro posicional

Você pode identificar um parâmetro posicional na ***command_name ?*** saída do comando. Um parâmetro posicional tem colchetes em torno do nome do parâmetro, em um dos seguintes formatos:

- [*-parameter_name parameter_value*] mostra um parâmetro necessário que é posicional.
- [*-parameter_name*[*parameter_value*] mostra um parâmetro opcional que é posicional.

Por exemplo, quando exibido como o seguinte na ***command_name ?*** saída, o parâmetro é posicional para o comando em que aparece:

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

No entanto, quando exibido como o seguinte, o parâmetro é não posicional para o comando em que aparece:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Exemplos de uso de parâmetros posicionais

No exemplo a seguir, a ***volume create ?*** saída mostra que três parâmetros são posicionais para o comando: `-volume` `-aggregate` , E `-size`.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

No exemplo a seguir, o `volume create` comando é especificado sem tirar vantagem da funcionalidade do parâmetro posicional:

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

Os exemplos a seguir usam a funcionalidade de parâmetro posicional para aumentar a eficiência da entrada de comando. Os parâmetros posicionais são intercalados com parâmetros não posicionais no `volume create` comando, e os valores dos parâmetros posicionais são especificados sem os nomes dos parâmetros. Os parâmetros posicionais são especificados na mesma sequência indicada pela **`volume create ?`** saída. Ou seja, o valor para `-volume` é especificado antes do `-aggregate` de , que por sua vez é especificado antes do de `-size`.

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0

cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

Métodos de acesso a páginas man do ONTAP

As páginas de manual do ONTAP (man) explicam como usar os comandos do ONTAP CLI. Essas páginas estão disponíveis na linha de comando e também são publicadas em *referências de comando* específicas da versão.

Na linha de comando ONTAP, use o `man command_name` comando para exibir a página manual do comando especificado. Se você não especificar um nome de comando, o índice de página manual será exibido. Você pode usar o `man man` comando para exibir informações sobre o `man` próprio comando. Pode sair de uma página de manual introduzindo **`q`**.

Consulte o Referência de comando para a sua versão do ONTAP 9 para saber mais sobre os comandos ONTAP de nível de administrador e de nível avançado disponíveis na sua versão.

Gerenciar sessões de CLI

Você pode gravar uma sessão CLI em um arquivo com um limite de nome e tamanho especificado e, em seguida, fazer o upload do arquivo para um destino FTP ou HTTP. Você também pode exibir ou excluir arquivos nos quais você gravou sessões CLI anteriormente.

Grave uma sessão CLI

Um Registro de uma sessão CLI termina quando você interrompe a gravação ou termina a sessão CLI, ou quando o arquivo atinge o limite de tamanho especificado. O limite de tamanho padrão do arquivo é de 1 MB. O limite máximo de tamanho do arquivo é de 2 GB.

Gravar uma sessão CLI é útil, por exemplo, se você estiver solucionando um problema e quiser salvar informações detalhadas ou se quiser criar um Registro permanente de uso de espaço em um determinado momento.

Passos

1. Comece a gravar a sessão CLI atual em um arquivo:

   ```
   system script start
   ```

   Para obter mais informações sobre como usar o `system script start` comando, consulte a página de manual.

   O ONTAP começa a gravar sua sessão CLI no arquivo especificado.

2. Prossiga com sua sessão CLI.
3. Quando terminar, pare de gravar a sessão:

   ```
   system script stop
   ```

   Para obter mais informações sobre como usar o `system script stop` comando, consulte a página de manual.

   O ONTAP pára de gravar sua sessão CLI.

Comandos para gerenciar Registros de sessões CLI

Você usa os `system script` comandos para gerenciar Registros de sessões CLI.

Se você quiser…	Use este comando…
Comece a gravar a sessão CLI atual em um arquivo especificado	`system script start`
Pare de gravar a sessão CLI atual	`system script stop`

Se você quiser…	Use este comando…
Exibir informações sobre Registros de sessões CLI	`system script show`
Carregue um Registro de uma sessão CLI para um destino FTP ou HTTP	`system script upload`
Excluir um Registro de uma sessão CLI	`system script delete`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar o período de tempo limite automático das sessões CLI

O valor de tempo limite especifica por quanto tempo uma sessão CLI permanece inativa antes de ser terminada automaticamente. O valor de tempo limite da CLI é de todo o cluster. Ou seja, cada nó em um cluster usa o mesmo valor de tempo limite da CLI.

Por padrão, o período de tempo limite automático das sessões CLI é de 30 minutos.

Você usa os `system timeout` comandos para gerenciar o período de tempo limite automático das sessões CLI.

Se você quiser…	Use este comando…
Exibir o período de tempo limite automático para sessões CLI	`system timeout show`
Modifique o período de tempo limite automático para sessões CLI	`system timeout modify`

Informações relacionadas

"Referência do comando ONTAP"

Gerenciamento de clusters (somente administradores de cluster)

Exibir informações sobre os nós em um cluster

Você pode exibir nomes de nós, se os nós estão íntegros e se eles estão qualificados para participar do cluster. No nível de privilégio avançado, você também pode exibir se um nó contém epsilon.

Passos

1. Para exibir informações sobre os nós em um cluster, use o `cluster show` comando.

   Se você quiser que a saída mostre se um nó possui epsilon, execute o comando no nível de privilégio avançado.

Exemplos de exibição dos nós em um cluster

O exemplo a seguir exibe informações sobre todos os nós em um cluster de quatro nós:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

O exemplo a seguir exibe informações detalhadas sobre o nó chamado "'node1" no nível de privilégio avançado:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

Exibir atributos do cluster

Você pode exibir o identificador exclusivo de um cluster (UUID), nome, número de série, localização e informações de Contato.

Passos

1. Para exibir os atributos de um cluster, use o `cluster identity show` comando.

Exemplo de exibição de atributos de cluster

O exemplo a seguir exibe o nome, o número de série, a localização e as informações de Contato de um cluster.

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

Modifique os atributos do cluster

Você pode modificar os atributos de um cluster, como o nome do cluster, o local e as informações de Contato, conforme necessário.

Sobre esta tarefa

Não é possível alterar o UUID de um cluster, que é definido quando o cluster é criado.

Passos

1. Para modificar atributos de cluster, use o `cluster identity modify` comando.

   O `-name` parâmetro especifica o nome do cluster. A `cluster identity modify` página man descreve as regras para especificar o nome do cluster.

   O `-location` parâmetro especifica a localização do cluster.

   O `-contact` parâmetro especifica as informações de Contato, como um nome ou endereço de e-mail.

Exemplo de renomeação de um cluster

O comando a seguir renomeia o cluster atual ("'cluster1') para "'cluster2'":

```
cluster1::> cluster identity modify -name cluster2
```

Exibir o status dos anéis de replicação do cluster

Você pode exibir o status dos anéis de replicação do cluster para ajudar a diagnosticar problemas em todo o cluster. Se o cluster tiver problemas, a equipe de suporte poderá solicitar que você execute esta tarefa para ajudar nos esforços de solução de problemas.

Passos

1. Para exibir o status dos anéis de replicação do cluster, use o `cluster ring show` comando no nível de privilégio avançado.

Exemplo de exibição do status de replicação do anel do cluster

O exemplo a seguir exibe o status do anel de replicação VLDB em um nó chamado node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

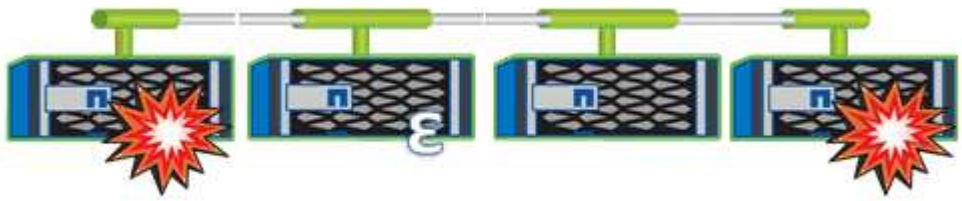
Sobre quórum e epsilon

O quórum e o epsilon são medidas importantes de integridade e função do cluster que, em conjunto, indicam como os clusters abordam potenciais desafios de comunicação e conetividade.

Quorum é uma pré-condição para um cluster totalmente funcional. Quando um cluster está no quórum, uma maioria simples dos nós é saudável e pode se comunicar uns com os outros. Quando o quorum é perdido, o cluster perde a capacidade de realizar operações normais de cluster. Apenas uma coleção de nós pode ter quórum de cada vez, porque todos os nós compartilham coletivamente uma única visualização dos dados. Portanto, se dois nós não-comunicantes forem permitidos modificar os dados de maneiras divergentes, não será mais possível reconciliar os dados em uma única visualização de dados.

Cada nó no cluster participa de um protocolo de votação que elege um nó *master*; cada nó restante é um *secondary*. O nó principal é responsável pela sincronização de informações no cluster. Quando o quórum é formado, ele é mantido por votação contínua. Se o nó mestre ficar offline e o cluster ainda estiver no quórum, um novo mestre será eleito pelos nós que permanecem online.

Como existe a possibilidade de um empate em um cluster que tem um número par de nós, um nó tem um peso de votação fracionário extra chamado *epsilon*. Se a conetividade entre duas partes iguais de um cluster grande falhar, o grupo de nós que contêm epsilon mantém quórum, assumindo que todos os nós estão saudáveis. Por exemplo, a ilustração a seguir mostra um cluster de quatro nós no qual dois dos nós falharam. No entanto, como um dos nós sobreviventes possui epsilon, o cluster permanece no quórum, embora não haja uma maioria simples de nós saudáveis.



O Epsilon é atribuído automaticamente ao primeiro nó quando o cluster é criado. Se o nó que mantém o epsilon não estiver saudável, assumir o seu parceiro de alta disponibilidade ou for assumido pelo parceiro de alta disponibilidade, o epsilon será reatribuído automaticamente a um nó saudável em um par de HA diferente.

Colocar um nó off-line pode afetar a capacidade do cluster de permanecer no quorum. Portanto, o ONTAP emite uma mensagem de aviso se você tentar uma operação que irá tirar o cluster do quórum ou então colocar uma interrupção longe de uma perda de quórum. Você pode desativar as mensagens de aviso de quórum usando o `cluster quorum-service options modify` comando no nível avançado de privilégio.

Em geral, assumindo uma conetividade confiável entre os nós do cluster, um cluster maior é mais estável do que um cluster menor. O requisito de quórum de uma maioria simples de metade dos nós mais o epsilon é mais fácil de manter em um cluster de 24 nós do que em um cluster de dois nós.

Um cluster de dois nós apresenta alguns desafios únicos para manter o quórum. Os clusters de dois nós usam *cluster HA*, no qual nenhum nó detém epsilon; em vez disso, ambos os nós são continuamente polled para garantir que, se um nó falhar, o outro tem acesso completo de leitura e gravação aos dados, bem como acesso a interfaces lógicas e funções de gerenciamento.

Quais são os volumes do sistema

Os volumes do sistema são volumes do FlexVol que contêm metadados especiais, como metadados para logs de auditoria de serviços de arquivo. Esses volumes ficam visíveis no cluster para que você possa considerar totalmente o uso do storage no cluster.

Os volumes de sistema pertencem ao servidor de gerenciamento de cluster (também chamado de administrador SVM) e são criados automaticamente quando a auditoria de serviços de arquivos é ativada.

Você pode visualizar volumes do sistema usando o `volume show` comando, mas a maioria das outras operações de volume não são permitidas. Por exemplo, você não pode modificar um volume de sistema usando o `volume modify` comando.

Este exemplo mostra quatro volumes de sistema no SVM admin, que foram criados automaticamente quando a auditoria de serviços de arquivo foi ativada para um SVM de dados no cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

Gerenciar nós

Adicione nós ao cluster

Depois que um cluster é criado, você pode expandi-lo adicionando nós a ele. Você adiciona apenas um nó de cada vez.

O que você vai precisar

- Se você estiver adicionando nós a um cluster de vários nós, todos os nós existentes no cluster devem estar íntegros (indicado pela `cluster show`).
- Se estiver adicionando nós a um cluster sem switch de dois nós, você deverá converter seu cluster sem switch de dois nós para um cluster conetado ao switch usando um switch de cluster compatível com NetApp.

  A funcionalidade de cluster sem switch é suportada apenas em um cluster de dois nós.

- Se você estiver adicionando um segundo nó a um cluster de nó único, o segundo nó deve ter sido instalado e a rede de cluster deve ter sido configurada.
- Se o cluster tiver a configuração automática do SP ativada, a sub-rede especificada para o SP deve ter recursos disponíveis para permitir que o nó de junção use a sub-rede especificada para configurar automaticamente o SP.
- Você deve ter reunido as seguintes informações para o LIF de gerenciamento de nós do novo nó:
  - Porta
  - Endereço IP
  - Máscara de rede
  - Gateway predefinido

Sobre esta tarefa

Os nós precisam estar em números pares para que possam formar pares de HA. Depois de começar a adicionar um nó ao cluster, você deve concluir o processo. O nó deve fazer parte do cluster antes de poder começar a adicionar outro nó.

Passos

1. Ligue o nó que você deseja adicionar ao cluster.

   O nó é inicializado e o assistente de configuração do nó é iniciado no console.

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.

   Enter the node management interface port [e0M]:
   ```

2. Saia do assistente de configuração do nó: `exit`

   O assistente de configuração do nó é encerrado e é apresentado um aviso de início de sessão, avisando que não concluiu as tarefas de configuração.

3. Inicie sessão na conta de administrador utilizando o `admin` nome de utilizador.
4. Inicie o assistente Configuração do cluster:

   `cluster setup`

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

Para obter mais informações sobre como configurar um cluster usando a GUI de configuração, consulte a "System Manager" ajuda on-line.

5. Pressione Enter para usar a CLI para concluir esta tarefa. Quando for solicitado a criar um novo cluster ou ingressar em um existente, digite **`join`**.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

Se a versão do ONTAP em execução no novo nó for diferente da versão em execução no cluster existente, o sistema informará um `System checks Error: Cluster join operation cannot be performed at this time` erro. Este é o comportamento esperado. Para continuar, execute o `add-node -allow-mixed-version-join new_node_name` comando no nível de privilégio avançado a partir de um nó existente no cluster.

6. Siga as instruções para configurar o nó e associá-lo ao cluster:
   - Para aceitar o valor padrão de um prompt, pressione Enter.
   - Para inserir seu próprio valor para um prompt, digite o valor e pressione Enter.
7. Repita as etapas anteriores para cada nó adicional que você deseja adicionar.

Depois de terminar

Depois de adicionar nós ao cluster, ative o failover de storage para cada par de HA.

Informações relacionadas

"Clusters ONTAP de versão mista"

Remova os nós do cluster

Você pode remover nós indesejados de um cluster, um nó de cada vez. Depois de remover um nó, você também deve remover o parceiro de failover. Se você estiver removendo um nó, seus dados ficarão inacessíveis ou apagados.

Antes de começar

As condições a seguir devem ser satisfeitas antes de remover nós do cluster:

- Mais da metade dos nós no cluster precisa estar saudável.
- Todos os dados no nó que você deseja remover devem ter sido evacuados.
  - Isso pode incluir "limpando dados de um volume criptografado".
- Todos os volumes que não são raiz "movido"foram de agregados pertencentes ao nó.
- Todos os agregados que não são root foram "eliminado"do nó.
- Se o nó possuir discos FIPS (Federal Information Processing Standards) ou SEDs (Self-Encrypting Disks)"a criptografia de disco foi removida", retornando os discos para o modo desprotegido.
  - Você também pode querer "Higienizar unidades FIPS ou SEDs".
- Os LIFs de dados foram "eliminado" ou "relocado" do nó.
- As LIFs de gerenciamento de cluster foram "relocado"do nó e as portas iniciais foram alteradas.
- Todos os LIFs entre clusters foram "removido".
  - Ao remover LIFs entre clusters, é exibido um aviso que pode ser ignorado.
- O failover de storage "desativado"foi para o nó.
- Todas as regras de failover de LIF foram "modificado" para remover portas no nó.
- Todas as VLANs no nó foram "eliminado".
- Se você tiver LUNs no nó a ser removido, você deve "Modifique a lista de nós de relatório do mapa LUN seletivo (SLM)" antes de remover o nó.

  Se você não remover o nó e seu parceiro de HA da lista de nós de relatórios do SLM, o acesso às LUNs anteriormente no nó poderá ser perdido mesmo que os volumes que contêm as LUNs tenham sido movidos para outro nó.

Recomenda-se que você emita uma mensagem do AutoSupport para notificar o suporte técnico da NetApp de que a remoção do nó está em andamento.

> Não é necessário executar operações como `cluster remove-node` , `cluster unjoin node rename` e quando uma atualização automática do ONTAP estiver em andamento.

Sobre esta tarefa

- Se você estiver executando um cluster de versão mista, poderá remover o último nó de versão baixa usando um dos comandos de privilégio avançados que começam com ONTAP 9.3:
  - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9 .4 e posterior: `cluster remove-node -skip-last-low-version-node-check`
- Se você desmarcar 2 nós de um cluster de 4 nós, o HA do cluster será automaticamente ativado nos dois nós restantes.

Todos os dados do sistema e do usuário, de todos os discos conetados ao nó, devem ficar inacessíveis aos usuários antes de remover um nó do cluster. Se um nó foi desvinculado incorretamente de um cluster, entre em Contato com o suporte da NetApp para obter assistência com opções de recuperação.

Passos

1. Altere o nível de privilégio para avançado:

```
set -privilege advanced
```

2. Verifique se um nó no cluster contém epsilon:

```
cluster show -epsilon true
```

3. Se um nó no cluster contiver epsilon e esse nó for desvinculado, mova o epsilon para um nó que não será desconetado:
   a. Mova o epsilon do nó que vai ser desconetado

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

   b. Mova o epsilon para um nó que não vai ser desconetado:

```
cluster modify -node <node_name> -epsilon true
```

4. Identificar o nó principal atual:

```
cluster ring show
```

   O nó principal é o nó que detém processos como "mgmt", "vldb", "vifmgr", "bcomd" e "crs".

5. Se o nó que você deseja remover for o nó principal atual, habilite outro nó no cluster a ser eleito como o nó mestre:
   a. Torne inelegível o nó principal atual para participar no cluster:

```
cluster modify -node <node_name> -eligibility false
```

   Quando o nó mestre se torna inelegível, um dos nós restantes é eleito pelo quorum do cluster como o novo mestre.

   b. Torne o nó principal anterior elegível para participar novamente no cluster:

```
cluster modify -node <node_name> -eligibility true
```

6. Faça login no LIF de gerenciamento de nós remoto ou no LIF de gerenciamento de cluster em um nó diferente daquele que está sendo removido.
7. Remova o nó do cluster:

Para esta versão ONTAP…	Use este comando…
ONTAP 9,3	`cluster unjoin`
ONTAP 9 .4 e mais tarde	`cluster remove-node*`

Se você tiver um cluster de versão mista e estiver removendo o último nó de versão inferior, use o `-skip -last-low-version-node-check` parâmetro com esses comandos.

O sistema informa-o do seguinte:

- Você também deve remover o parceiro de failover do nó do cluster.
- Depois que o nó é removido e antes que ele possa reingressar em um cluster, você deve usar a opção de menu de inicialização (4) Limpar configuração e inicializar todos os discos ou a opção (9) Configurar particionamento de unidade avançado para apagar a configuração do nó e inicializar todos os discos.

  Uma mensagem de falha é gerada se você tiver condições que devem ser endereçadas antes de remover o nó. Por exemplo, a mensagem pode indicar que o nó tem recursos compartilhados que você deve remover ou que o nó está em uma configuração de HA de cluster ou configuração de failover de storage que você deve desativar.

Se o nó for o mestre do quórum, o cluster perderá brevemente e retornará ao quórum. Essa perda de quorum é temporária e não afeta nenhuma operação de dados.

8. Se uma mensagem de falha indicar condições de erro, aborde essas condições e execute novamente o `cluster remove-node` comando ou `cluster unjoin`.

   O nó é reinicializado automaticamente depois de removido com sucesso do cluster.

9. Se você estiver reutilizando o nó, apague a configuração do nó e inicialize todos os discos:
   a. Durante o processo de inicialização, pressione Ctrl-C para exibir o menu de inicialização quando solicitado a fazê-lo.
   b. Selecionar a opção do menu de arranque (4) Limpar a configuração e inicializar todos os discos.
10. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

11. Repita as etapas anteriores para remover o parceiro de failover do cluster.

Acesse os arquivos de log, despejo de memória e MIB de um nó usando um navegador da Web

O (`spi`serviço da Web Service Processor Infrastructure) está habilitado por padrão para permitir que um navegador da Web acesse os arquivos de log, despejo de núcleo e MIB de um nó no cluster. Os arquivos permanecem acessíveis mesmo quando o nó está inativo, desde que o nó seja assumido pelo parceiro.

O que você vai precisar

- O LIF de gerenciamento de clusters deve estar ativo.

  Você pode usar o LIF de gerenciamento do cluster ou de um nó para acessar o `spi` serviço da Web. No entanto, é recomendável usar o LIF de gerenciamento de cluster.

  O `network interface show` comando exibe o status de todas as LIFs no cluster.

- Você deve usar uma conta de usuário local para acessar o `spi` serviço da Web, as contas de usuário de domínio não são suportadas.
- Se a sua conta de usuário não tiver a função "admin" (que tem acesso ao `spi` serviço da Web por padrão), sua função de controle de acesso deve ter acesso ao `spi` serviço da Web.

  O `vserver services web access show` comando mostra quais funções têm acesso a quais serviços da Web.

- Se você não estiver usando a conta de usuário "'admin'" (que inclui o `http` método de acesso por padrão), sua conta de usuário deve ser configurada com o `http` método de acesso.

  O `security login show` comando mostra os métodos de acesso e login das contas de usuário e suas funções de controle de acesso.

- Se você quiser usar HTTPS para acesso seguro à Web, o SSL deve estar habilitado e um certificado digital deve ser instalado.

  O `system services web show` comando exibe a configuração do mecanismo de protocolo da Web no nível do cluster.

Sobre esta tarefa

O `spi` serviço da Web está ativado por predefinição e o serviço pode ser desativado manualmente (`vserver services web modify -vserver * -name spi -enabled false`).

A função "'admin'" tem acesso ao `spi` serviço web por padrão e o acesso pode ser desativado manualmente (`services web access delete -vserver` *`cluster_name`* `-name spi -role admin`).

Passos

1. Aponte o navegador da Web para o `spi` URL do serviço da Web em um dos seguintes formatos:

   - `http://`*`cluster-mgmt-LIF`*`/spi/`
   - `https://`*`cluster-mgmt-LIF`*`/spi/`

     `cluster-mgmt-LIF` É o endereço IP do LIF de gerenciamento de cluster.

2. Quando solicitado pelo navegador, insira sua conta de usuário e senha.

   Depois que a conta for autenticada, o navegador exibirá links para os `/mroot/etc/log/` diretórios , `/mroot/etc/crash/` e `/mroot/etc/mib/` de cada nó no cluster.

Acesse o console do sistema de um nó

Se um nó estiver suspenso no menu de inicialização ou no prompt do ambiente de inicialização, você poderá acessá-lo somente pelo console do sistema (também chamado de *console serial*). Você pode acessar o console do sistema de um nó a partir de uma conexão SSH para o SP do nó ou para o cluster.

Sobre esta tarefa

Tanto o SP quanto o ONTAP oferecem comandos que permitem acessar o console do sistema. No entanto, a partir do SP, você pode acessar apenas o console do sistema de seu próprio nó. No cluster, você pode acessar o console do sistema de qualquer nó no cluster.

Passos

1. Acesse o console do sistema de um nó:

Se você está no…	Digite este comando…
CLI do SP do nó	`system console`
CLI do ONTAP	`system node run-console`

2. Inicie sessão na consola do sistema quando lhe for pedido que o faça.
3. Para sair do console do sistema, pressione Ctrl-D.

Exemplos de acesso ao console do sistema

O exemplo a seguir mostra o resultado da inserção `system console` do comando no prompt "'SP node2'". O console do sistema indica que o node2 está suspenso no prompt do ambiente de inicialização. O `boot_ontap` comando é inserido no console para inicializar o nó no ONTAP. Ctrl-D é então pressionado para sair do console e retornar ao SP.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

(Ctrl-D é pressionado para sair do console do sistema.)

```
Connection to 123.12.123.12 closed.
SP node2>
```

O exemplo a seguir mostra o resultado de inserir o `system node run-console` comando do ONTAP para acessar o console do sistema do node2, que está pendurado no prompt do ambiente de inicialização. O `boot_ontap` comando é inserido no console para inicializar o node2 no ONTAP. Ctrl-D é então pressionado para sair do console e retornar ao ONTAP.

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

(Ctrl-D é pressionado para sair do console do sistema.)

```
Connection to 123.12.123.12 closed.
cluster1::>
```

Gerenciar volumes de raiz de nós e agregados de raiz

O volume raiz de um nó é um FlexVol volume instalado na fábrica ou pelo software de configuração. Ele é reservado para arquivos de sistema, arquivos de log e arquivos principais. O nome do diretório é `/mroot`, que é acessível somente através do systemshell pelo suporte técnico. O tamanho mínimo para o volume raiz de um nó depende do modelo da plataforma.

Regras que regem os volumes de raiz dos nós e a visão geral dos agregados de raiz

O volume raiz de um nó contém diretórios e arquivos especiais para esse nó. O agregado raiz contém o volume raiz. Algumas regras governam o volume raiz e o agregado raiz de um nó.

- As seguintes regras regem o volume raiz do nó:
  - A menos que o suporte técnico o instrua a fazê-lo, não modifique a configuração ou o conteúdo do volume raiz.
  - Não armazene dados do usuário no volume raiz.

    Armazenar dados de usuário no volume raiz aumenta o tempo de giveback de storage entre nós em um par de HA.

  - Você pode mover o volume raiz para outro agregado. [relocate-root]Consulte .
- O agregado raiz é dedicado apenas ao volume raiz do nó.

  O ONTAP impede que você crie outros volumes no agregado raiz.

"NetApp Hardware Universe"

Libere espaço no volume raiz de um nó

Uma mensagem de aviso aparece quando o volume raiz de um nó ficou cheio ou quase cheio. O nó não pode funcionar corretamente quando seu volume raiz está cheio. Você pode liberar espaço no volume raiz de um nó excluindo arquivos de despejo de núcleo, arquivos de rastreamento de pacotes e cópias Snapshot de volume raiz.

Passos

1. Exiba os arquivos de despejo de núcleo do nó e seus nomes:

   ```
   system node coredump show
   ```

2. Excluir arquivos indesejados de despejo de memória do nó:

   ```
   system node coredump delete
   ```

3. Acesse o nodeshell:

   `system node run -node` *`nodename`*

   `nodename` é o nome do nó cujo espaço de volume raiz você deseja liberar.

4. Mude para o nível de privilégio avançado nodeshell a partir do nodeshell:

priv set advanced

5. Exiba e exclua os arquivos de rastreamento de pacotes do nó através do nodeshell:
   a. Exibir todos os arquivos no volume raiz do nó:

      ls /etc

   b. Se algum arquivo de rastreamento de pacote (`*.trc`) estiver no volume raiz do nó, exclua-os individualmente:

      rm /etc/log/packet_traces/*file_name.trc*

6. Identifique e exclua as cópias Snapshot do volume raiz do nó através do nodeshell:
   a. Identifique o nome do volume raiz:

      vol status

      O volume raiz é indicado pela palavra "root" na coluna "Opções" da `vol status` saída do comando.

      No exemplo a seguir, o volume raiz é `vol0`:

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

   a. Exibir cópias Snapshot do volume raiz:

      snap list root_vol_name

   b. Excluir cópias snapshot do volume raiz indesejadas:

      snap delete root_vol_namesnapshot_name

7. Saia do nodeshell e volte para a concha:

   exit

Realocar volumes raiz para novos agregados

O procedimento de substituição de raiz migra o agregado de raiz atual para outro conjunto de discos sem interrupção.

Sobre esta tarefa

O failover de armazenamento deve estar habilitado para realocar volumes raiz. Você pode usar o `storage failover modify -node *nodename* -enable true` comando para ativar o failover.

Você pode alterar o local do volume raiz para um novo agregado nos seguintes cenários:

- Quando os agregados de raiz não estão no disco que preferir
- Quando pretender reorganizar os discos ligados ao nó
- Quando estiver a efetuar uma substituição de prateleira das prateleiras de disco EOS

Passos

1. Defina o nível de privilégio como avançado:

   `set privilege advanced`

2. Realocar o agregado raiz:

   `system node migrate-root -node` *`nodename`* `-disklist` *`disklist`* `-raid-type` *`raid-type`*

   - **-node**

     Especifica o nó que possui o agregado raiz que você deseja migrar.

   - **-disklist**

     Especifica a lista de discos nos quais o novo agregado raiz será criado. Todos os discos precisam ser sobressalentes e de propriedade do mesmo nó. O número mínimo de discos necessário depende do tipo RAID.

   - **-raid-type**

     Especifica o tipo RAID do agregado raiz. O valor padrão é `raid-dp`.

3. Monitorize o progresso do trabalho:

   `job show -id` *`jobid`* `-instance`

Resultados

Se todas as pré-verificações forem bem-sucedidas, o comando iniciará uma tarefa de substituição de volume raiz e será encerrado. Espere que o nó seja reiniciado.

Iniciar ou parar uma visão geral do nó

Talvez seja necessário iniciar ou parar um nó por motivos de manutenção ou solução de problemas. Você pode fazer isso a partir da CLI do ONTAP, do prompt do ambiente de inicialização ou da CLI do SP.

O uso do comando SP CLI `system power off` ou `system power cycle` para desligar ou desligar um nó pode causar um desligamento inadequado do nó (também chamado de *desligamento anormal*) e não substitui um desligamento gracioso usando o comando ONTAP `system node halt`.

Reinicie um nó no prompt do sistema

Você pode reinicializar um nó no modo normal a partir do prompt do sistema. Um nó é configurado para inicializar a partir do dispositivo de inicialização, como uma placa CompactFlash do PC.

Passos

1. Se o cluster contiver quatro ou mais nós, verifique se o nó a ser reiniciado não possui epsilon:

   a. Defina o nível de privilégio como avançado:

      set -privilege advanced

   b. Determine qual nó contém o epsilon:

      cluster show

      O exemplo a seguir mostra que "'node1" contém epsilon:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   a. Se o nó a ser reinicializado contiver epsilon, remova o epsilon do nó:

      cluster modify -node *node_name* -epsilon false

   b. Atribua o epsilon a um nó diferente que permanecerá ativo:

      cluster modify -node *node_name* -epsilon true

   c. Voltar ao nível de privilégio de administrador:

      set -privilege admin

2. Use o `system node reboot` comando para reinicializar o nó.

   Se você não especificar o `-skip-lif-migration` parâmetro, o comando tentará migrar dados e LIFs de gerenciamento de cluster de forma síncrona para outro nó antes da reinicialização. Se a migração de LIF falhar ou expirar, o processo de reinicialização será abortado e o ONTAP exibirá um erro para indicar a falha de migração de LIF.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

   O nó inicia o processo de reinicialização. O prompt de login do ONTAP é exibido, indicando que o processo de reinicialização está concluído.

Inicie o ONTAP no prompt do ambiente de inicialização

Você pode inicializar a versão atual ou a versão de backup do ONTAP quando estiver no prompt do ambiente de inicialização de um nó.

Passos

1. Acesse o prompt do ambiente de inicialização a partir do prompt do sistema de armazenamento usando o `system node halt` comando.

   O console do sistema de armazenamento exibe o prompt do ambiente de inicialização.

2. No prompt do ambiente de inicialização, digite um dos seguintes comandos:

Para iniciar…	Digite…
A versão atual do ONTAP	`boot_ontap`
A imagem primária do ONTAP a partir do dispositivo de arranque	`boot_primary`
A imagem de cópia de segurança do ONTAP a partir do dispositivo de arranque	`boot_backup`

   Se você não tiver certeza sobre qual imagem usar, você deve usar `boot_ontap` na primeira instância.

Encerre um nó

Você pode encerrar um nó se ele ficar sem resposta ou se a equipe de suporte o direcionar para fazer isso como parte dos esforços de solução de problemas.

Passos

1. Se o cluster contiver quatro ou mais nós, verifique se o nó a ser desligado não possui epsilon:

   a. Defina o nível de privilégio como avançado:

      `set -privilege advanced`

   b. Determine qual nó contém o epsilon:

      `cluster show`

      O exemplo a seguir mostra que "'node1" contém epsilon:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   a. Se o nó a ser desligado mantiver o epsilon, remova o epsilon do nó:

```
cluster modify -node node_name -epsilon false
```

b. Atribua o epsilon a um nó diferente que permanecerá ativo:

```
cluster modify -node node_name -epsilon true
```

c. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

2. Use o `system node halt` comando para encerrar o nó.

   Se você não especificar o `-skip-lif-migration` parâmetro, o comando tentará migrar dados e LIFs de gerenciamento de cluster de forma síncrona para outro nó antes do desligamento. Se a migração de LIF falhar ou expirar o tempo, o processo de encerramento é cancelado e o ONTAP exibe um erro para indicar a falha de migração de LIF.

   Você pode acionar manualmente um despejo de memória com o desligamento usando ambos os `-dump` parâmetros.

   O exemplo a seguir desliga o nó chamado "'node1" para manutenção de hardware:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

Gerencie um nó usando o menu de inicialização

Você pode usar o menu de inicialização para corrigir problemas de configuração em um nó, redefinir a senha de administrador, inicializar discos, redefinir a configuração do nó e restaurar as informações de configuração do nó de volta para o dispositivo de inicialização.

> Se um par de HA estiver usando "Criptografia de unidades SAS ou NVMe (SED, NSE, FIPS)", siga as instruções no "Retornar uma unidade FIPS ou SED para o modo desprotegido"tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Passos

1. Reinicie o nó para acessar o menu de inicialização usando o `system node reboot` comando no prompt do sistema.

   O nó inicia o processo de reinicialização.

2. Durante o processo de reinicialização, pressione Ctrl-C para exibir o menu de inicialização quando solicitado a fazê-lo.

   O nó exibe as seguintes opções para o menu de inicialização:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

Opção de menu de inicialização (2) a inicialização sem /etc/rc é obsoleta e não tem efeito no sistema.

3. Selecione uma das seguintes opções inserindo o número correspondente:

Para…	Selecione…
Continue a inicializar o nó no modo normal	1) bota normal
Altere a senha do nó, que também é a senha da conta "admin"	3) altere a senha

Para…	Selecione…
Inicialize os discos do nó e crie um volume raiz para o nó	4) limpe a configuração e inicialize todos os discos Esta opção de menu apaga todos os dados nos discos do nó e redefine a configuração do nó para as configurações padrão de fábrica. Selecione este item de menu apenas depois de o nó ter sido removido de um cluster (não associado) e não ser Unido a outro cluster. Para um nó com compartimentos de disco internos ou externos, o volume raiz nos discos internos é inicializado. Se não houver compartimentos de disco internos, o volume raiz nos discos externos será inicializado. Para um sistema que executa a virtualização FlexArray com compartimentos de disco internos ou externos, os LUNs do array não são inicializados. Todos os discos nativos em compartimentos internos ou externos são inicializados. Para um sistema que executa a virtualização FlexArray apenas com LUNS de array e sem compartimentos de disco internos ou externos, o volume raiz nos LUNS de storage array é inicializado, consulte "A instalar o FlexArray". Se o nó que você deseja inicializar tiver discos particionados para particionamento de dados raiz, os discos devem ser desparticionados antes que o nó possa ser inicializado, consulte **9) Configurar particionamento de unidade avançado** e "Gerenciamento de discos e agregados".
Execute operações de manutenção de disco e agregado e obtenha informações detalhadas sobre o agregado e o disco.	5) Inicialização do modo de manutenção Você sai do modo Manutenção usando o `halt` comando.
Restaure as informações de configuração do volume raiz do nó para o dispositivo de inicialização, como um cartão CompactFlash do PC	6) Atualizar flash a partir da configuração de backup O ONTAP armazena algumas informações de configuração de nós no dispositivo de inicialização. Quando o nó é reiniciado, as informações no dispositivo de inicialização são automaticamente gravadas no volume raiz do nó. Se o dispositivo de inicialização ficar corrompido ou precisar ser substituído, você deve usar essa opção de menu para restaurar as informações de configuração do volume raiz do nó de volta para o dispositivo de inicialização.

Para…	Selecione…
Instale um novo software no nó	7) instale primeiro novo software Se o software ONTAP no dispositivo de inicialização não incluir suporte para o storage array que você deseja usar para o volume raiz, você poderá usar essa opção de menu para obter uma versão do software compatível com seu storage array e instalá-lo no nó. Esta opção de menu é apenas para instalar uma versão mais recente do software ONTAP em um nó que não tem volume raiz instalado. *Não* Use esta opção de menu para atualizar o ONTAP.
Reinicie o nó	8) nó de reinicialização

Desparticionar todos os discos e remover suas informações de propriedade ou limpar a configuração e inicializar o sistema com discos inteiros ou particionados	9) Configurar particionamento de unidade avançado
	
	A partir do ONTAP 9.2, a opção particionamento de unidade avançado fornece recursos de gerenciamento adicionais para discos que são configurados para particionamento de dados raiz ou dados raiz. As seguintes opções estão disponíveis na opção de inicialização 9:
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

Exibir atributos do nó

Você pode exibir os atributos de um ou mais nós no cluster, por exemplo, o nome, proprietário, local, número do modelo, número de série, quanto tempo o nó está sendo executado, estado de integridade e elegibilidade para participar de um cluster.

Passos

1. Para exibir os atributos de um nó especificado ou sobre todos os nós em um cluster, use o `system node show` comando.

Exemplo de exibição de informações sobre um nó

O exemplo a seguir exibe informações detalhadas sobre o node1:

```
cluster1::> system node show -node node1
                           Node: node1
                          Owner: Eng IT
                       Location: Lab 5
                          Model: model_number
                  Serial Number: 12345678
                      Asset Tag: -
                         Uptime: 23 days 04:42
                NVRAM System ID: 118051205
                      System ID: 0118051205
                         Vendor: NetApp
                         Health: true
                    Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

Modificar atributos de nó

Você pode modificar os atributos de um nó conforme necessário. Os atributos que você pode modificar incluem as informações de proprietário do nó, informações de localização, etiqueta de ativo e elegibilidade para participar do cluster.

Sobre esta tarefa

A elegibilidade de um nó para participar no cluster pode ser modificada no nível de privilégio avançado usando o `-eligibility` parâmetro do `system node modify` comando ou `cluster modify`. Se você definir a elegibilidade de um nó como `false`, o nó ficará inativo no cluster.

> Não é possível modificar a elegibilidade do nó localmente. Ele deve ser modificado de um nó diferente. A elegibilidade do nó também não pode ser modificada com uma configuração de HA do cluster.

> Você deve evitar definir a elegibilidade de um nó para `false`, exceto para situações como restaurar a configuração do nó ou manutenção prolongada do nó. O acesso a dados SAN e nas ao nó pode ser afetado quando o nó não é elegível.

Passos

1. Use o `system node modify` comando para modificar os atributos de um nó.

Exemplo de modificação de atributos de nó

O comando a seguir modifica os atributos do nó "'node1". O proprietário do nó está definido como "'Joe Smith'" e sua etiqueta de ativo está definida como "'js1234'":

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

Renomeie um nó

Você pode alterar o nome de um nó conforme necessário.

Passos

1. Para renomear um nó, use o `system node rename` comando.

   O `-newname` parâmetro especifica o novo nome para o nó. A `system node rename` página man descreve as regras para especificar o nome do nó.

   Se você quiser renomear vários nós no cluster, você deve executar o comando para cada nó individualmente.

   O nome do nó não pode ser "'tudo'" porque "'tudo'" é um nome reservado ao sistema.

Exemplo de renomeação de um nó

O seguinte comando renomeia o nó "'node1" para "'node1a":

```
cluster1::> system node rename -node node1 -newname node1a
```

Gerenciar clusters de nó único

Um cluster de nó único é uma implementação especial de um cluster executado em um nó autônomo. Os clusters de nó único não são recomendados porque não fornecem redundância. Se o nó ficar inativo, o acesso aos dados será perdido.

Para tolerância de falhas e operações ininterruptas, é altamente recomendável configurar seu cluster com "Alta disponibilidade (pares de HA)"o .

Se você optar por configurar ou atualizar um cluster de nó único, você deve estar ciente do seguinte:

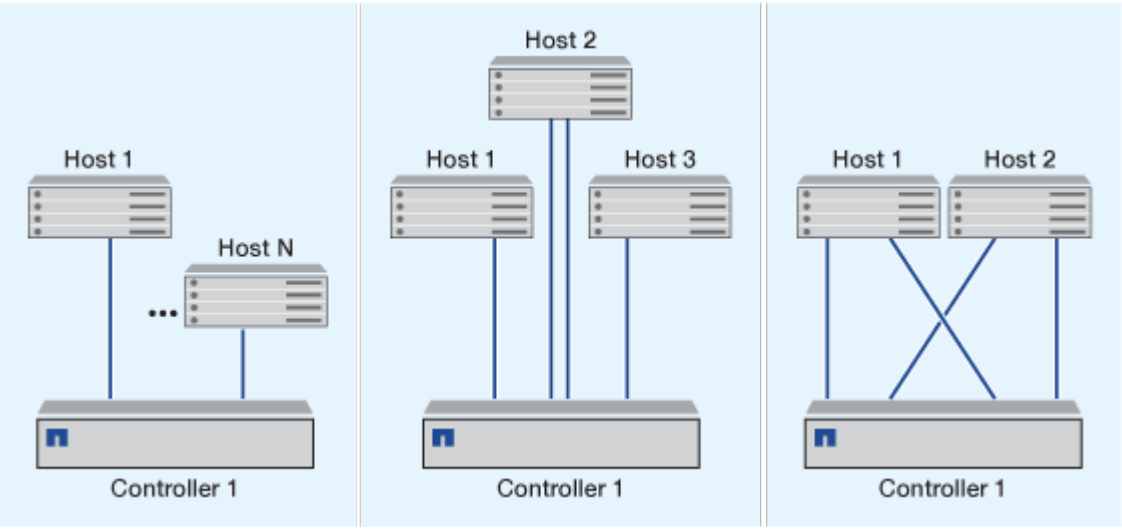
- A criptografia de volume raiz não é compatível com clusters de nó único.
- Se você remover nós para ter um cluster de nó único, modifique as portas do cluster para servir o tráfego de dados, modificando as portas do cluster para serem portas de dados e criando LIFs de dados nas portas de dados.
- Para clusters de nó único, você pode especificar o destino do backup de configuração durante a configuração do software. Após a configuração, essas configurações podem ser modificadas usando comandos ONTAP.
- Se houver vários hosts conetados ao nó, cada host pode ser configurado com um sistema operacional diferente, como Windows ou Linux. Se houver vários caminhos do host para o controlador, o ALUA deve estar habilitado no host.

Maneiras de configurar hosts SAN iSCSI com nós únicos

Você pode configurar hosts SAN iSCSI para se conetar diretamente a um único nó ou para se conetar através de um ou mais switches IP. O nó pode ter várias conexões iSCSI ao switch.

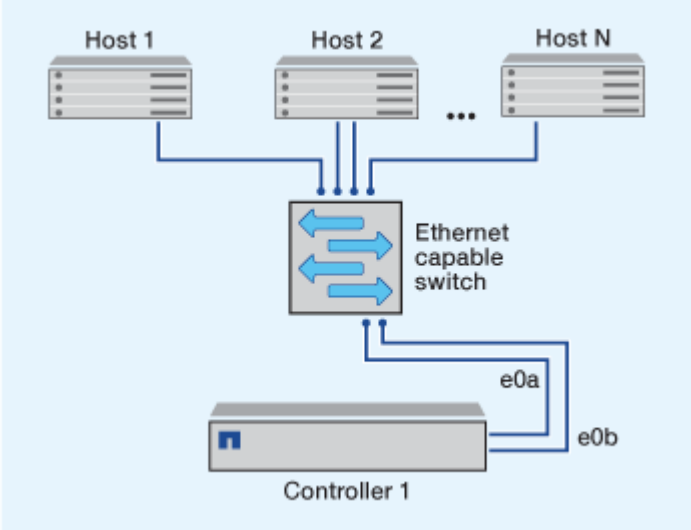
Configurações de nó único com conexão direta

Nas configurações de nó único com conexão direta, um ou mais hosts são conectados diretamente ao nó.



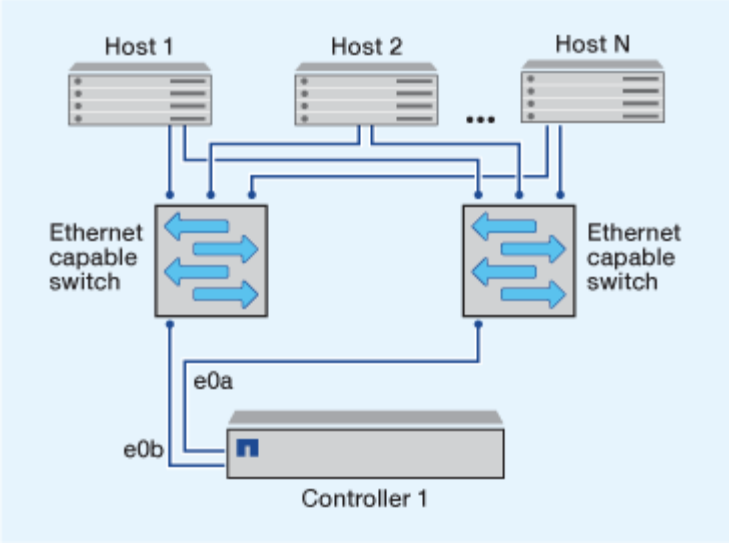
Configurações de nó único de rede única

Em configurações de nó único de rede única, um switch coneta um único nó a um ou mais hosts. Como há um único switch, essa configuração não é totalmente redundante.



Configurações de nó único multi-rede

Em configurações de nó único de várias redes, dois ou mais switches conetam um único nó a um ou mais hosts. Como existem vários switches, essa configuração é totalmente redundante.



Maneiras de configurar hosts SAN FC e FC-NVMe com nós únicos

É possível configurar hosts SAN FC e FC-NVMe com nós únicos por meio de uma ou mais malhas. O NPIV (N-Port ID Virtualization) é necessário e deve ser ativado em todos os switches FC na malha. Não é possível conectar diretamente hosts SAN FC ou FC-NMVE a nós únicos sem usar um switch FC.

Configurações de nó único de malha única

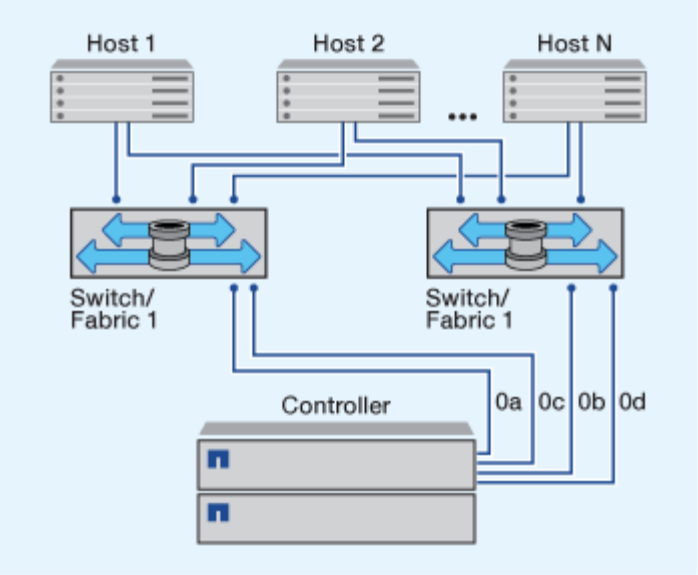
Nas configurações de nó único de estrutura única, há um switch que conecta um único nó a um ou mais hosts. Como há um único switch, essa configuração não é totalmente redundante.

Em configurações de nó único de malha única, o software de multipathing não é necessário se você tiver apenas um caminho único do host para o nó.

Configurações de nó único de MultiFabric

Nas configurações de nó único de várias estruturas, há dois ou mais switches que conectam um único nó a um ou mais hosts. Para simplificar, a figura a seguir mostra uma configuração de nó único de várias malhas com apenas duas malhas. No entanto, você pode ter duas ou mais malhas em qualquer configuração de várias malhas. Nesta figura, o controlador de armazenamento é montado no chassi superior e o chassi inferior pode estar vazio ou pode ter um módulo IOMX, como acontece neste exemplo.

As portas de destino FC (0a, 0C, 0b, 0d) nas ilustrações são exemplos. Os números reais das portas variam dependendo do modelo do nó de armazenamento e se você está usando adaptadores de expansão.



Informações relacionadas

"Relatório técnico da NetApp 4684: Implementando e configurando SANs modernas com NVMe-of"

Atualização do ONTAP para cluster de nó único

A partir do ONTAP 9.2, você pode usar a CLI do ONTAP para executar uma atualização automatizada de um cluster de nó único. Como os clusters de nó único não têm redundância, as atualizações são sempre disruptivas. As atualizações disruptivas não podem ser realizadas usando o System Manager.

Antes de começar

Você deve concluir as etapas de atualização"preparação".

Passos

1. Elimine o pacote de software ONTAP anterior:

```
cluster image package delete -version <previous_package_version>
```

2. Faça o download do pacote de software ONTAP de destino:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

3. Verifique se o pacote de software está disponível no repositório de pacotes de cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.7              M/DD/YYYY 10:32:15
```

4. Verifique se o cluster está pronto para ser atualizado:

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7

WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Monitorize o progresso da validação:

```
cluster image show-update-progress
```

6. Conclua todas as ações necessárias identificadas pela validação.
7. Opcionalmente, gere uma estimativa de atualização de software:

```
cluster image update -version <package_version_number> -estimate-only
```

A estimativa de atualização de software exibe detalhes sobre cada componente a ser atualizado e a duração estimada da atualização.

8. Execute a atualização de software:

```
cluster image update -version <package_version_number>
```

Se for encontrado um problema, a atualização será interrompida e solicitará que você tome medidas corretivas. Você pode usar o comando show-update-progress da imagem de cluster para exibir detalhes sobre quaisquer problemas e o andamento da atualização. Depois de corrigir o problema, você pode retomar a atualização usando o comando de retomada-atualização da imagem de cluster.

9. Apresentar o progresso da atualização do cluster:

```
cluster image show-update-progress
```

O nó é reinicializado como parte da atualização e não pode ser acessado durante a reinicialização.

10. Acionar uma notificação:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

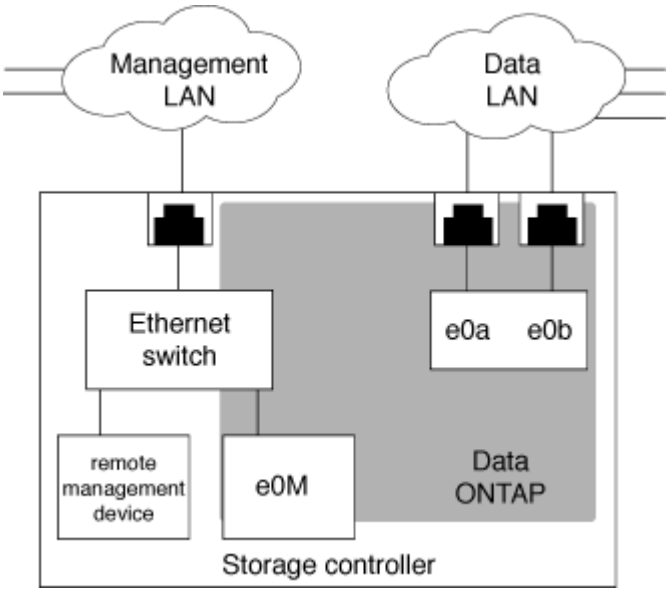
Se o cluster não estiver configurado para enviar mensagens, uma cópia da notificação será salva localmente.

Configure a rede SP/BMC

Isolar o tráfego de rede de gerenciamento

É uma prática recomendada configurar o SP/BMC e a interface de gerenciamento e0M em uma sub-rede dedicada ao tráfego de gerenciamento. A execução do tráfego de dados pela rede de gerenciamento pode causar degradação do desempenho e problemas de roteamento.

A porta Ethernet de gerenciamento na maioria dos controladores de armazenamento (indicada por um ícone de chave na parte traseira do chassi) é conetada a um switch Ethernet interno. O switch interno fornece conetividade ao SP/BMC e à interface de gerenciamento e0M, que você pode usar para acessar o sistema de armazenamento através de protocolos TCP/IP como Telnet, SSH e SNMP.



Se pretende utilizar o dispositivo de gestão remota e o e0M, tem de os configurar na mesma sub-rede IP. Como essas são interfaces de baixa largura de banda, a prática recomendada é configurar SP/BMC e e0M em uma sub-rede dedicada ao tráfego de gerenciamento.

Se não conseguir isolar o tráfego de gestão ou se a sua rede de gestão dedicada for invulgarmente grande, deve tentar manter o volume de tráfego de rede o mais baixo possível. O tráfego de broadcast ou multicast de

entrada excessiva pode degradar o desempenho do SP/BMC.

Alguns controladores de storage, como o AFF A800, têm duas portas externas, uma para BMC e outra para e0M. Para esses controladores, não há nenhum requisito para configurar BMC e e0M na mesma sub-rede IP.

Considerações para a configuração de rede SP/BMC

Pode ativar a configuração automática de rede no nível do cluster para o SP (recomendado). Você também pode deixar a configuração automática de rede do SP desativada (o padrão) e gerenciar a configuração de rede do SP manualmente no nível do nó. Existem algumas considerações para cada caso.

Este tópico aplica-se tanto ao SP como ao BMC.

A configuração automática de rede SP permite que o SP use recursos de endereço (incluindo o endereço IP, máscara de sub-rede e endereço de gateway) da sub-rede especificada para configurar sua rede automaticamente. Com a configuração automática de rede SP, não é necessário atribuir manualmente endereços IP para o SP de cada nó. Por padrão, a configuração automática de rede do SP está desativada; isso ocorre porque a ativação da configuração exige que a sub-rede a ser usada para a configuração seja definida primeiro no cluster.

Se você ativar a configuração automática de rede do SP, os seguintes cenários e considerações serão aplicados:

- Se o SP nunca tiver sido configurado, a rede SP é configurada automaticamente com base na sub-rede especificada para a configuração automática de rede SP.
- Se o SP foi configurado manualmente anteriormente ou se a configuração de rede SP existente for baseada em uma sub-rede diferente, a rede SP de todos os nós do cluster será reconfigurada com base na sub-rede especificada na configuração automática de rede SP.

  A reconfiguração pode resultar na atribuição de um endereço diferente ao SP, o que pode ter um impactos na configuração de DNS e na capacidade de resolver nomes de host do SP. Como resultado, você pode precisar atualizar sua configuração de DNS.

- Um nó que se une ao cluster usa a sub-rede especificada para configurar sua rede SP automaticamente.
- O `system service-processor network modify` comando não permite alterar o endereço IP do SP.

  Quando a configuração automática de rede SP está ativada, o comando permite-lhe ativar ou desativar a interface de rede SP.

  - Se a configuração automática de rede do SP tiver sido ativada anteriormente, a desativação da interface de rede do SP resulta na liberação do recurso de endereço atribuído e retornada à sub-rede.
  - Se você desabilitar a interface de rede SP e reativá-la, o SP poderá ser reconfigurado com um endereço diferente.

Se a configuração automática de rede do SP estiver desativada (o padrão), os seguintes cenários e considerações serão aplicados:

- Se o SP nunca tiver sido configurado, a configuração de rede do SP IPv4 é predefinida para utilizar DHCP IPv4 e IPv6 é desativada.

Um nó que une o cluster também usa DHCP IPv4 para sua configuração de rede SP por padrão.

- O `system service-processor network modify` comando permite configurar o endereço IP SP de um nó.

  É apresentada uma mensagem de aviso quando tenta configurar manualmente a rede SP com endereços atribuídos a uma sub-rede. Ignorar o aviso e prosseguir com a atribuição manual de endereços pode resultar em um cenário com endereços duplicados.

Se a configuração automática de rede do SP for desativada depois de ter sido ativada anteriormente, aplicam-se os seguintes cenários e considerações:

- Se a configuração automática de rede do SP tiver a família de endereços IPv4 desativada, a rede SP IPv4 é predefinida para utilizar DHCP e o `system service-processor network modify` comando permite modificar a configuração do SP IPv4 para nós individuais.
- Se a configuração automática de rede do SP tiver a família de endereços IPv6 desativada, a rede do SP IPv6 também será desativada e o `system service-processor network modify` comando permitirá ativar e modificar a configuração do SP IPv6 para nós individuais.

Ative a configuração automática de rede SP/BMC

É preferível ativar o SP para utilizar a configuração automática de rede em vez de configurar manualmente a rede SP. Como a configuração automática de rede do SP é de todo o cluster, você não precisa gerenciar manualmente a rede SP para nós individuais.

Esta tarefa aplica-se tanto ao SP como ao BMC.

- A sub-rede que você deseja usar para a configuração automática de rede SP já deve estar definida no cluster e não deve ter conflitos de recursos com a interface de rede SP.

  O `network subnet show` comando exibe informações de sub-rede para o cluster.

  O parâmetro que força a associação de sub-rede (o `-force-update-lif-associations` parâmetro `network subnet` dos comandos) é suportado apenas em LIFs de rede e não na interface de rede SP.

- Se você quiser usar conexões IPv6 para o SP, o IPv6 já deve estar configurado e habilitado para o ONTAP.

  O `network options ipv6 show` comando exibe o estado atual de IPv6 configurações para ONTAP.

Passos

1. Especifique a família de endereços IPv4 ou IPv6 e o nome da sub-rede que você deseja que o SP use usando o `system service-processor network auto-configuration enable` comando.
2. Apresentar a configuração automática da rede SP utilizando o `system service-processor network auto-configuration show` comando.
3. Se, posteriormente, pretender desativar ou reativar a interface de rede SP IPv4 ou IPv6 para todos os nós que estão em quórum, utilize o `system service-processor network modify` comando com os `-address-family` [`true`|`false`` parâmetros [`IPv4`|`IPv6`] e `-enable`].

   Quando a configuração automática de rede do SP está ativada, não é possível modificar o endereço IP do

SP para um nó que está no quórum. Só pode ativar ou desativar a interface de rede SP IPv4 ou IPv6.

Se um nó estiver fora do quórum, você poderá modificar a configuração de rede SP do nó, incluindo o endereço IP do SP, executando `system service-processor network modify` a partir do nó e confirmando que deseja substituir a configuração automática de rede do SP para o nó. No entanto, quando o nó se junta ao quórum, a reconfiguração automática do SP ocorre para o nó com base na sub-rede especificada.

Configure a rede SP/BMC manualmente

Se não tiver a configuração automática de rede configurada para o SP, tem de configurar manualmente a rede SP de um nó para que o SP possa ser acessível utilizando um endereço IP.

O que você vai precisar

Se você quiser usar conexões IPv6 para o SP, o IPv6 já deve estar configurado e habilitado para o ONTAP. Os `network options ipv6` comandos gerenciam IPv6 configurações para o ONTAP.

Esta tarefa aplica-se tanto ao SP como ao BMC.

Você pode configurar o SP para usar IPv4, IPv6 ou ambos. A configuração do SP IPv4 suporta endereçamento estático e DHCP, e a configuração do SP IPv6 suporta somente endereçamento estático.

Se a configuração automática de rede SP tiver sido configurada, não será necessário configurar manualmente a rede SP para nós individuais e o `system service-processor network modify` comando permite ativar ou desativar apenas a interface de rede SP.

Passos

1. Configure a rede SP para um nó usando o `system service-processor network modify` comando.
   - O `-address-family` parâmetro especifica se a configuração IPv4 ou IPv6 do SP deve ser modificada.
   - O `-enable` parâmetro permite a interface de rede da família de endereços IP especificada.
   - O `-dhcp` parâmetro especifica se deve-se usar a configuração de rede do servidor DHCP ou o endereço de rede fornecido.

     Só pode ativar o DHCP (definindo `-dhcp` para `v4`) se estiver a utilizar o IPv4. Não é possível ativar o DHCP para configurações IPv6.
   - O `-ip-address` parâmetro especifica o endereço IP público para o SP.

     É apresentada uma mensagem de aviso quando tenta configurar manualmente a rede SP com endereços atribuídos a uma sub-rede. Ignorar o aviso e prosseguir com a atribuição de endereço manual pode resultar em uma atribuição de endereço duplicado.
   - O `-netmask` parâmetro especifica a máscara de rede para o SP (se estiver usando IPv4.)
   - O `-prefix-length` parâmetro especifica o tamanho do prefixo da rede da máscara de sub-rede para o SP (se estiver usando IPv6.)
   - O `-gateway` parâmetro especifica o endereço IP do gateway para o SP.
2. Configure a rede SP para os nós restantes no cluster repetindo a etapa 1.

3. Exiba a configuração da rede SP e verifique o status da configuração do SP usando o `system service-processor network show` comando com os `-instance` parâmetros ou `-field setup-status`.

   O status de configuração do SP para um nó pode ser um dos seguintes:

   - `not-setup` — não configurado
   - `succeeded` — Configuração bem-sucedida
   - `in-progress` — Configuração em andamento
   - `failed` — a configuração falhou

Exemplo de configuração da rede SP

O exemplo a seguir configura o SP de um nó para usar o IPv4, ativa o SP e exibe a configuração de rede SP para verificar as configurações:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

Modifique a configuração do serviço da API do SP

A API SP é uma API de rede segura que permite que o ONTAP se comunique com o SP pela rede. Você pode alterar a porta usada pelo serviço de API do SP, renovar os certificados que o serviço usa para comunicação interna ou desativar o serviço totalmente. Você precisa modificar a configuração somente em situações raras.

Sobre esta tarefa

- O serviço de API do SP usa a porta `50000` por padrão.

  Você pode alterar o valor da porta se, por exemplo, estiver em uma configuração de rede em que a porta `50000` é usada para comunicação por outro aplicativo de rede ou se quiser diferenciar entre o tráfego de outros aplicativos e o tráfego gerado pelo serviço de API do SP.

- Os certificados SSL e SSH usados pelo serviço API SP são internos ao cluster e não são distribuídos externamente.

  No caso improvável de os certificados estarem comprometidos, você pode renová-los.

- O serviço de API do SP está habilitado por padrão.

  Você só precisa desativar o serviço de API SP em situações raras, como em uma LAN privada onde o SP não esteja configurado ou usado e você deseja desativar o serviço.

  Se o serviço de API do SP estiver desativado, a API não aceita conexões de entrada. Além disso, a funcionalidade, como atualizações de firmware SP baseadas em rede e a coleção de logs do "sistema próprio" do SP baseada em rede, torna-se indisponível. O sistema muda para utilizando a interface de série.

Passos

1. Mude para o nível de privilégio avançado utilizando o `set -privilege advanced` comando.
2. Modifique a configuração do serviço API do SP:

Se você quiser…	Use o seguinte comando…
Altere a porta usada pelo serviço de API do SP	`system service-processor api-service modify` com o `-port` {`49152`.`65535`parâmetro

Se você quiser…	Use o seguinte comando…
Renove os certificados SSL e SSH usados pelo serviço API SP para comunicação interna	• Para ONTAP 9.5 ou posterior utilização `system service-processor api-service renew-internal-certificate` • Para ONTAP 9 .4 e uso anterior • `system service-processor api-service renew-certificates` Se nenhum parâmetro for especificado, somente os certificados de host (incluindo os certificados de cliente e servidor) serão renovados. Se o `-renew-all true` parâmetro for especificado, os certificados de host e o certificado de CA raiz serão renovados.
comm	
Desative ou reative o serviço de API do SP	`system service-processor api-service modify` com o `-is-enabled {true`

3. Exiba a configuração do serviço API SP usando o `system service-processor api-service show` comando.

Gerencie nós remotamente usando o SP/BMC

Gerencie um nó remotamente usando a visão geral do SP/BMC

Você pode gerenciar um nó remotamente usando um controlador integrado, chamado de processador de Serviço (SP) ou controlador de gerenciamento de placa base (BMC). Este controlador de gerenciamento remoto está incluído em todos os modelos de plataforma atuais. O controlador permanece operacional independentemente do estado operacional do nó.

As seguintes plataformas suportam BMC em vez de SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800
- AFF A700s
- AFF A400
- AFF A320
- AFF A220

- AFF C190

Sobre o SP

O processador de serviço (SP) é um dispositivo de gerenciamento remoto que permite acessar, monitorar e solucionar problemas remotamente de um nó.

Os principais recursos do SP incluem o seguinte:

- O SP permite que você acesse um nó remotamente para diagnosticar, desligar, desligar ou reinicializar o nó, independentemente do estado do controlador do nó.

  O SP é alimentado por uma tensão de espera, que está disponível desde que o nó tenha energia de entrada de pelo menos uma de suas fontes de alimentação.

  Você pode fazer login no SP usando um aplicativo cliente Shell seguro de um host de administração. Em seguida, você pode usar a CLI do SP para monitorar e solucionar problemas do nó remotamente. Além disso, você pode usar o SP para acessar o console serial e executar comandos ONTAP remotamente.

  Você pode acessar o SP a partir do console serial ou acessar o console serial a partir do SP. O SP permite abrir simultaneamente uma sessão de CLI do SP e uma sessão de console separada.

  Por exemplo, quando um sensor de temperatura se torna criticamente alto ou baixo, o ONTAP aciona o SP para desligar a placa-mãe graciosamente. O console serial fica sem resposta, mas você ainda pode pressionar Ctrl-G no console para acessar a CLI do SP. Em seguida, você pode usar o `system power on` comando ou `system power cycle` do SP para ligar ou desligar o nó.

- O SP monitora sensores ambientais e Registra eventos para ajudá-lo a tomar ações de serviço oportunas e eficazes.

  O SP monitora sensores ambientais, como as temperaturas do nó, tensões, correntes e velocidades do ventilador. Quando um sensor ambiental atinge uma condição anormal, o SP Registra as leituras anormais, notifica o ONTAP do problema e envia alertas e notificações de "sistema próprio" conforme necessário por meio de uma mensagem AutoSupport, independentemente de o nó poder enviar mensagens AutoSupport.

  O SP também Registra eventos como progresso da inicialização, alterações na Unidade substituível em Campo (FRU), eventos gerados pelo ONTAP e histórico de comandos do SP. Você pode invocar manualmente uma mensagem do AutoSupport para incluir os arquivos de log do SP coletados de um nó especificado.

  Além de gerar essas mensagens em nome de um nó inativo e anexar informações de diagnóstico adicionais a mensagens AutoSupport, o SP não tem efeito na funcionalidade AutoSupport. As configurações do AutoSupport e o comportamento do conteúdo da mensagem são herdadas do ONTAP.

  > O SP não depende da `-transport` configuração de parâmetro do `system node autosupport modify` comando para enviar notificações. O SP usa apenas o protocolo SMTP (Simple Mail Transport Protocol) e requer a configuração AutoSupport do host para incluir informações do host de e-mail.

  Se o SNMP estiver ativado, o SP gera traps SNMP para hosts de intercetação configurados para todos os eventos de "sistema próprio".

- O SP tem um buffer de memória não volátil que armazena até 4.000 eventos em um log de eventos do

sistema (SEL) para ajudá-lo a diagnosticar problemas.

O SEL armazena cada entrada de log de auditoria como um evento de auditoria. Ele é armazenado na memória flash integrada no SP. A lista de eventos do SEL é enviada automaticamente pelo SP para destinatários especificados por meio de uma mensagem do AutoSupport.

O SEL contém as seguintes informações:

- Eventos de hardware detetados pelo SP - por exemplo, status do sensor sobre fontes de alimentação, tensão ou outros componentes
- Erros detetados pelo SP—por exemplo, um erro de comunicação, uma falha de ventilador ou um erro de memória ou CPU
- Eventos críticos de software enviados para o SP pelo nó - por exemplo, um pânico, uma falha de comunicação, uma falha de inicialização ou um "sistema próprio" acionado pelo usuário como resultado da emissão do SP `system reset` ou `system power cycle` comando

- O SP monitora o console serial, independentemente de os administradores estarem conetados ou conetados ao console.

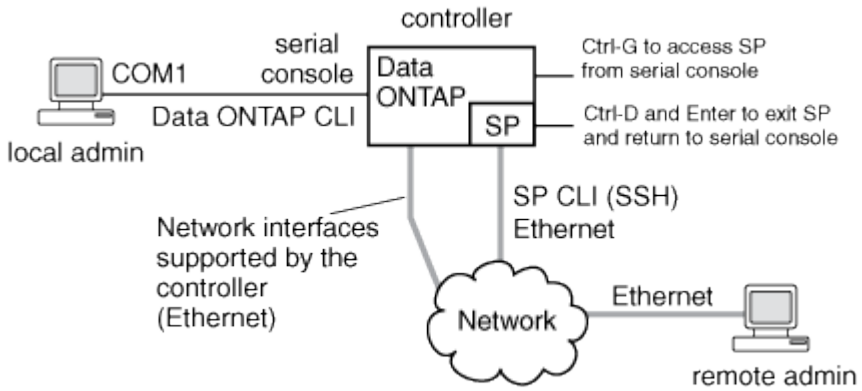
  Quando as mensagens são enviadas para o console, o SP as armazena no log do console. O log do console persiste enquanto o SP tiver energia de qualquer uma das fontes de alimentação do nó. Como o SP funciona com energia em espera, ele permanece disponível mesmo quando o nó é ligado ou desligado.

- A aquisição assistida por hardware está disponível se o SP estiver configurado.
- O serviço API SP permite que o ONTAP se comunique com o SP pela rede.

  O serviço aprimora o gerenciamento do ONTAP do SP, oferecendo suporte a funcionalidades baseadas em rede, como o uso da interface de rede para a atualização de firmware do SP, permitindo que um nó acesse a funcionalidade do SP ou o console do sistema de outro nó e faça o upload do log do SP de outro nó.

  Você pode modificar a configuração do serviço API SP alterando a porta que o serviço usa, renovando os certificados SSL e SSH que são usados pelo serviço para comunicação interna ou desativando o serviço completamente.

O diagrama a seguir ilustra o acesso ao ONTAP e ao SP de um nó. A interface SP é acessada através da porta Ethernet (indicada por um ícone de chave na parte traseira do chassi):



O que o Baseboard Management Controller faz

A partir do ONTAP 9.1, em determinadas plataformas de hardware, o software é personalizado para suportar um novo controlador integrado chamado controlador de gerenciamento de placa base (BMC). O BMC tem comandos de interface de linha de comando (CLI) que você pode usar para gerenciar o dispositivo remotamente.

O BMC funciona de forma semelhante ao processador de Serviço (SP) e usa muitos dos mesmos comandos. O BMC permite que você faça o seguinte:

- Configure as definições de rede BMC.
- Acesse um nó remotamente e execute tarefas de gerenciamento de nós, como diagnosticar, desligar, desligar e reiniciar o nó.

Existem algumas diferenças entre o SP e o BMC:

- O BMC controla completamente a monitorização ambiental dos elementos de alimentação, dos elementos de refrigeração, dos sensores de temperatura, dos sensores de tensão e dos sensores de corrente. O BMC comunica as informações do sensor ao ONTAP através do IPMI.
- Alguns dos comandos de alta disponibilidade (HA) e armazenamento são diferentes.
- O BMC não envia mensagens AutoSupport.

Atualizações automáticas de firmware também estão disponíveis ao executar o ONTAP 9.2 GA ou posterior com os seguintes requisitos:

- A revisão 1,15 ou posterior do firmware do BMC deve ser instalada.

  É necessária uma atualização manual para atualizar o firmware do BMC de 1,12 para 1,15 ou posterior.

- O BMC reinicia automaticamente após a conclusão de uma atualização de firmware.

  As operações do nó não são afetadas durante uma reinicialização do BMC.

Métodos de gerenciamento de atualizações de firmware do SP/BMC

O ONTAP inclui uma imagem de firmware do SP que é chamada de *imagem de linha de base*. Se uma nova versão do firmware do SP ficar disponível posteriormente, você tem a opção de baixá-lo e atualizar o firmware do SP para a versão baixada sem atualizar a versão do ONTAP.

Este tópico aplica-se tanto ao SP como ao BMC.

O ONTAP oferece os seguintes métodos para gerenciar atualizações de firmware do SP:

- A funcionalidade de atualização automática do SP está ativada por predefinição, permitindo que o firmware do SP seja atualizado automaticamente nos seguintes cenários:
  - Quando você atualiza para uma nova versão do ONTAP

O processo de atualização do ONTAP inclui automaticamente a atualização do firmware do SP, desde que a versão do firmware do SP fornecida com o ONTAP seja mais recente do que a versão do SP executada no nó.

> O ONTAP deteta uma atualização automática do SP com falha e aciona uma ação corretiva para tentar novamente a atualização automática do SP até três vezes. Se todas as três tentativas falharem, consulte o link do artigo da base de dados de Conhecimento: https://kb.NetApp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_os/Health_Monitor_SPAutoUpgradeFailedMajorAlert__SP AutoSupport_upgrade_Fails_-_AutoSupport_Message[Health Monitor SPAutoUpgradeFailed SP upgrade_Message].

- Quando você faz o download de uma versão do firmware do SP a partir do site de suporte da NetApp e a versão baixada é mais recente do que a versão que o SP está atualmente em execução
- Quando você faz o downgrade ou reverte para uma versão anterior do ONTAP

  O firmware do SP é atualizado automaticamente para a versão compatível mais recente que é suportada pela versão do ONTAP para a qual você reverteu ou baixou. Não é necessária uma atualização manual do firmware do SP.

Você tem a opção de desativar a funcionalidade de atualização automática do SP usando o `system service-processor image modify` comando. No entanto, é recomendável que você deixe a funcionalidade ativada. Desativar a funcionalidade pode resultar em combinações subótimas ou não qualificadas entre a imagem ONTAP e a imagem de firmware SP.

- O ONTAP permite acionar manualmente uma atualização do SP e especificar como a atualização deve ocorrer usando o `system service-processor image update` comando.

  Você pode especificar as seguintes opções:

  - O pacote de firmware do SP a utilizar (`-package`)

    Você pode atualizar o firmware do SP para um pacote baixado especificando o nome do arquivo do pacote. O comando ADVANCE `system image package show` exibe todos os arquivos de pacote (incluindo os arquivos do pacote de firmware do SP) que estão disponíveis em um nó.

  - Se deve usar o pacote de firmware SP de linha de base para a atualização do SP (`-baseline`)

    Você pode atualizar o firmware do SP para a versão de linha de base fornecida com a versão atual do ONTAP.

  > Se utilizar algumas das opções ou parâmetros de atualização mais avançados, as definições de configuração do BMC poderão ser temporariamente eliminadas. Após a reinicialização, o ONTAP pode levar até 10 minutos para restaurar a configuração do BMC.

- O ONTAP permite exibir o status da atualização de firmware SP mais recente acionada pelo ONTAP usando o `system service-processor image update-progress show` comando.

Qualquer ligação existente ao SP é terminada quando o firmware do SP está a ser atualizado. Este é o caso se a atualização do firmware do SP é acionada automaticamente ou manualmente.

Informações relacionadas

"Downloads do NetApp: Firmware e Diagnóstico do sistema"

Quando o SP/BMC utiliza a interface de rede para atualizações de firmware

Uma atualização de firmware do SP que é acionada a partir do ONTAP com o SP executando a versão 1,5, 2,5, 3,1 ou posterior suporta o uso de um mecanismo de transferência de arquivos baseado em IP através da interface de rede SP.

Este tópico aplica-se tanto ao SP como ao BMC.

Uma atualização de firmware do SP através da interface de rede é mais rápida do que uma atualização através da interface serial. Ele reduz a janela de manutenção durante a qual o firmware do SP está sendo atualizado e também não causa interrupções na operação do ONTAP. As versões do SP que suportam esse recurso estão incluídas no ONTAP. Eles também estão disponíveis no site de suporte da NetApp e podem ser instalados em controladores que executam uma versão compatível do ONTAP.

Quando você estiver executando o SP versão 1,5, 2,5, 3,1 ou posterior, os seguintes comportamentos de atualização de firmware se aplicam:

- Uma atualização de firmware do SP que é *automaticamente* acionada pelo ONTAP usa a interface de rede para a atualização; no entanto, a atualização automática do SP muda para usar a interface serial para a atualização de firmware se ocorrer uma das seguintes condições:
  - A interface de rede SP não está configurada ou não está disponível.
  - A transferência de arquivos baseada em IP falha.
  - O serviço de API do SP está desativado.

Independentemente da versão do SP que você está executando, uma atualização de firmware do SP acionada a partir da CLI do SP sempre usa a interface de rede do SP para a atualização.

Informações relacionadas

"Downloads do NetApp: Firmware e Diagnóstico do sistema"

Contas que podem acessar o SP

Ao tentar acessar o SP, você será solicitado a fornecer credenciais. As contas de usuários de cluster criadas com o `service-processor` tipo de aplicativo têm acesso à CLI do SP em qualquer nó do cluster. As contas de usuário do SP são gerenciadas a partir do ONTAP e autenticadas por senha. A partir do ONTAP 9.9,1, as contas de usuário do SP devem ter a `admin` função.

As contas de usuário para acessar o SP são gerenciadas a partir do ONTAP em vez da CLI do SP. Uma conta de usuário de cluster pode acessar o SP se ele for criado com o `-application` parâmetro do `security login create` comando definido como `service-processor` e o `-authmethod` parâmetro definido como `password`. O SP suporta apenas autenticação por palavra-passe.

Você deve especificar o `-role` parâmetro ao criar uma conta de usuário do SP.

- No ONTAP 9.9,1 e versões posteriores, você deve especificar `admin` para o `-role` parâmetro, e quaisquer modificações em uma conta exigem a `admin` função. Outras funções não são mais permitidas por motivos de segurança.
  - Se você estiver atualizando para o ONTAP 9.9,1 ou versões posteriores, "Alteração nas contas de usuário que podem acessar o processador de serviço"consulte .

    - Se você estiver revertendo para o ONTAP 9.8 ou versões anteriores, "Verifique as contas de usuário que podem acessar o processador de serviço"consulte .
- No ONTAP 9.8 e versões anteriores, qualquer função pode acessar o SP, mas `admin` é recomendado.

Por padrão, a conta de usuário do cluster chamada "admin" inclui o `service-processor` tipo de aplicativo e tem acesso ao SP.

O ONTAP impede que você crie contas de usuário com nomes que são reservados para o sistema (como "root" e "naroot"). Não é possível usar um nome reservado ao sistema para acessar o cluster ou o SP.

Você pode exibir as contas de usuário atuais do SP usando o `-application service-processor` parâmetro `security login show` do comando.

Acesse o SP/BMC de um host de administração

Você pode fazer login no SP de um nó de um host de administração para executar tarefas de gerenciamento de nós remotamente.

O que você vai precisar

Devem ser cumpridas as seguintes condições:

- O host de administração que você usa para acessar o SP deve oferecer suporte a SSHv2.
- Sua conta de usuário já deve estar configurada para acessar o SP.

  Para acessar o SP, sua conta de usuário deve ter sido criada com o `-application` parâmetro do `security login create` comando definido como `service-processor` e o `-authmethod` parâmetro definido como `password`.

Esta tarefa aplica-se tanto ao SP como ao BMC.

Se o SP estiver configurado para usar um endereço IPv4 ou IPv6 e se cinco tentativas de login SSH de um host falharem consecutivamente em 10 minutos, o SP rejeita solicitações de login SSH e suspende a comunicação com o endereço IP do host por 15 minutos. A comunicação é retomada após 15 minutos e você pode tentar fazer login no SP novamente.

O ONTAP impede que você crie ou use nomes reservados ao sistema (como "root" e "naroot") para acessar o cluster ou o SP.

Passos

1. No host de administração, faça login no SP:

   `ssh username@SP_IP_address`

2. Quando lhe for solicitado, introduza a palavra-passe `username` do .

   O prompt SP é exibido, indicando que você tem acesso à CLI do SP.

Exemplos de acesso à SP de um host de administração

O exemplo a seguir mostra como fazer login no SP com uma conta de usuário `joe` , que foi configurada para acessar o SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Os exemplos a seguir mostram como usar o endereço global IPv6 ou o endereço anunciado pelo roteador IPv6 para fazer login no SP em um nó que tenha SSH configurado para IPv6 e o SP configurado para IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Aceda ao SP/BMC a partir da consola do sistema

Você pode acessar o SP a partir do console do sistema (também chamado de *console serial*) para executar tarefas de monitoramento ou solução de problemas.

Sobre esta tarefa

Esta tarefa aplica-se tanto ao SP como ao BMC.

Passos

1. Acesse a CLI do SP a partir do console do sistema pressionando Ctrl-G no prompt.
2. Faça login na CLI do SP quando for solicitado.

   O prompt SP é exibido, indicando que você tem acesso à CLI do SP.

3. Saia da CLI do SP e retorne ao console do sistema pressionando Ctrl-D e pressione Enter.

Exemplo de acesso à CLI do SP a partir do console do sistema

O exemplo a seguir mostra o resultado de pressionar Ctrl-G do console do sistema para acessar a CLI do SP. O `help system power` comando é inserido no prompt do SP, seguido de Ctrl-D e Enter para retornar ao console do sistema.

```
cluster1::>
```

(Pressione Ctrl-G para acessar a CLI do SP.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Pressione Ctrl-D e Enter para retornar ao console do sistema.)

```
cluster1::>
```

Relação entre as sessões de CLI, console SP e console do sistema do SP

Você pode abrir uma sessão de CLI do SP para gerenciar um nó remotamente e abrir uma sessão de console SP separada para acessar o console do nó. A sessão do console SP espelha a saída exibida em uma sessão de console de sistema concorrente. O SP e o console do sistema têm ambientes de shell independentes com autenticação de login independente.

Entender como as sessões de CLI, console SP e console do sistema do SP estão relacionadas ajuda a gerenciar um nó remotamente. O seguinte descreve a relação entre as sessões:

- Somente um administrador pode fazer login na sessão da CLI do SP de cada vez. No entanto, o SP permite que você abra simultaneamente uma sessão da CLI do SP e uma sessão separada do console do SP.

  A CLI do SP é indicada com o prompt SP (`SP>`). A partir de uma sessão CLI do SP, você pode usar o comando SP `system console` para iniciar uma sessão de console do SP. Ao mesmo tempo, você pode iniciar uma sessão de CLI do SP separada por meio de SSH. Se você pressionar Ctrl-D para sair da sessão do console do SP, você retornará automaticamente à sessão da CLI do SP. Se uma sessão da CLI do SP já existir, uma mensagem pergunta se você deseja encerrar a sessão existente da CLI do SP. Se você digitar "'y'", a sessão CLI do SP existente será encerrada, permitindo que você retorne do console do SP para a CLI do SP. Esta ação é gravada no registo de eventos do SP.

  Em uma sessão da CLI do ONTAP conetada por meio de SSH, você pode alternar para o console do sistema de um nó executando o comando ONTAP `system node run-console` de outro nó.

- Por motivos de segurança, a sessão CLI do SP e a sessão do console do sistema têm autenticação de login independente.

  Quando você inicia uma sessão de console do SP a partir da CLI do SP (usando o comando SP `system console`), você será solicitado a fornecer a credencial do console do sistema. Ao acessar a CLI do SP a partir de uma sessão de console do sistema (pressionando Ctrl-G), você será solicitado a fornecer a credencial da CLI do SP.

- A sessão do console SP e a sessão do console do sistema têm ambientes de shell independentes.

  A sessão do console SP espelha a saída que é exibida em uma sessão de console de sistema concorrente. No entanto, a sessão simultânea do console do sistema não espelha a sessão do console do SP.

  A sessão do console SP não espelha a saída de sessões SSH simultâneas.

Gerencie os endereços IP que podem acessar o SP

Por padrão, o SP aceita solicitações de conexão SSH de hosts de administração de qualquer endereço IP. Você pode configurar o SP para aceitar solicitações de conexão SSH apenas dos hosts de administração que têm os endereços IP especificados. As alterações feitas se aplicam ao acesso SSH ao SP de qualquer nó no cluster.

Passos

1. Conceda acesso SP apenas aos endereços IP especificados usando o `system service-processor ssh add-allowed-addresses` comando com o `-allowed-addresses` parâmetro.
   - O valor do `-allowed-addresses` parâmetro deve ser especificado no formato de `address /netmask`, e vários `address/netmask` pares devem ser separados por vírgulas, por exemplo, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

     Definir o `-allowed-addresses` parâmetro para `0.0.0.0/0, ::/0` permite que todos os endereços IP acessem o SP (o padrão).
   - Quando você altera o padrão limitando o acesso à SP apenas aos endereços IP especificados, o ONTAP solicita que você confirme que deseja que os endereços IP especificados substituam a configuração padrão ""permitir tudo"" (`0.0.0.0/0, ::/0`).
   - O `system service-processor ssh show` comando exibe os endereços IP que podem acessar o SP.
2. Se você quiser impedir que um endereço IP especificado acesse o SP, use o `system service-processor ssh remove-allowed-addresses` comando com o `-allowed-addresses` parâmetro.

   Se você bloquear todos os endereços IP de acessar o SP, o SP se tornará inacessível de qualquer host de administração.

Exemplos de gerenciamento de endereços IP que podem acessar o SP

Os exemplos a seguir mostram a configuração padrão para o acesso SSH ao SP, altere o padrão limitando o acesso SP apenas aos endereços IP especificados, remova os endereços IP especificados da lista de acesso e, em seguida, restaure o acesso SP para todos os endereços IP:

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

Use a ajuda on-line na CLI do SP/BMC

A ajuda on-line exibe os comandos e opções da CLI do SP/BMC.

Sobre esta tarefa

Esta tarefa aplica-se tanto ao SP como ao BMC.

Passos

1. Para exibir informações de ajuda para os comandos SP/BMC, digite o seguinte:

Para acessar a ajuda do SP…	Para acessar a ajuda do BMC…
Digite `help` no prompt SP.	Digite `system` no prompt BMC.

O exemplo a seguir mostra a ajuda online da CLI do SP.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

O exemplo a seguir mostra a ajuda online da CLI do BMC.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. Para exibir informações de ajuda para a opção de um comando SP/BMC, digite `help` antes ou depois do comando SP/BMC.

   O exemplo a seguir mostra a ajuda online da CLI do SP para o comando SP `events`.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

O exemplo a seguir mostra a ajuda online da CLI do BMC para o comando BMC `system power`.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

Comandos para gerenciar um nó remotamente

Você pode gerenciar um nó remotamente acessando o SP e executando os comandos da CLI do SP para executar tarefas de gerenciamento de nós. Para várias tarefas de gerenciamento remoto de nós comumente executadas, você também pode usar comandos ONTAP de outro nó no cluster. Alguns comandos do SP são específicos da plataforma e podem não estar disponíveis na sua plataforma.

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
Exiba os comandos SP disponíveis ou subcomandos de um comando SP especificado	`help` [`command`]		
Exibir o nível de privilégio atual para a CLI do SP	`priv show`		
Defina o nível de privilégio para acessar o modo especificado para a CLI do SP	`priv set` {`admin`	`advanced`	`diag`
		Apresentar a data e a hora do sistema	`date`

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
	`date`	Exibir eventos registrados pelo SP	`events {all`
`info newest number`	`oldest number`		`search keyword`
		Exibir informações de status do SP e configuração da rede	`sp status[-v -d`
] A `-v` opção exibe estatísticas do SP em forma verbose. A `-d` opção adiciona o log de depuração do SP à tela.	`bmc status[-v -d`	] A `-v` opção exibe estatísticas do SP em forma verbose. A `-d` opção adiciona o log de depuração do SP à tela.	`system service-processor show`
Apresentar o período de tempo em que o SP esteve ativo e o número médio de trabalhos na fila de execução nos últimos 1, 5 e 15 minutos	`sp uptime`	`bmc uptime`	
Exiba os logs do console do sistema	`system log`		
Exiba os arquivos de log do SP ou os arquivos em um arquivo	`sp log history show[ -archive {latest {all` Selecionar		`archive-name] [-dump {all`
`file-name`	`bmc log history show[-archive {latest {all` Selecionar		`archive-name] [-dump {all`
`file-name`		Apresentar o estado de alimentação do controlador de um nó	`system power status`
	`system node power show`	Apresentar informações sobre a bateria	`system battery show`
		Apresentar informações ACP ou o estado dos sensores expansores	`system acp[show sensors show`

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
]			Listar todas as FRUs do sistema e suas IDs
`system fru list`			Exibir informações do produto para a FRU especificada
`system fru show fru_id`			Apresentar o registo do histórico de dados da FRU
`system fru log show` (nível de privilégio avançado)			Apresentar o estado dos sensores ambientais, incluindo os respetivos estados e valores atuais
`system sensors` ou `system sensors show`		`system node environment sensors show`	Apresentar o estado e os detalhes do sensor especificado
`system sensors get sensor_name` Pode obter `sensor_name` utilizando o `system sensors` comando ou `system sensors show`.			Exiba as informações da versão do firmware do SP
`version`		`system service-processor image show`	Exiba o histórico de comandos do SP
`sp log audit` (nível de privilégio avançado)	`bmc log audit`		Exiba as informações de depuração do SP
`sp log debug` (nível de privilégio avançado)	`bmc log debug` (nível de privilégio avançado)		Exiba o arquivo de mensagens do SP

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
`sp log messages` (nível de privilégio avançado)	`bmc log messages` (nível de privilégio avançado)		Apresentar as definições de recolha forense do sistema num evento de reposição do watchdog, apresentar as informações forenses do sistema recolhidas durante um evento de reposição do watchdog ou limpar as informações forenses do sistema recolhidas
`system forensics` [`show log dump`		`log clear`]	
	Inicie sessão na consola do sistema	`system console`	
`system node run-console`	Você deve pressionar Ctrl-D para sair da sessão do console do sistema.	Ligue ou desligue o nó ou execute um ciclo de alimentação (desligando e voltando a ligar)	`system power on`
	`system node power on` (nível de privilégio avançado)	`system power off`	
	`system power cycle`		

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
A alimentação em espera permanece ligada para manter o SP em funcionamento sem interrupção. Durante o ciclo de alimentação, ocorre uma breve pausa antes de ligar novamente a alimentação. Usar esses comandos para desligar ou desligar o nó pode causar um desligamento inadequado do nó (também chamado de *desligamento anormal*) e não substitui um desligamento gracioso usando o comando ONTAP `system node halt`.	Crie um despejo de núcleo e redefina o nó	`system core [-f]` A `-f` opção força a criação de um despejo de núcleo e a redefinição do nó.	

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
`system node coredump trigger` (nível de privilégio avançado)	Esses comandos têm o mesmo efeito que pressionar o botão de interrupção não masável (NMI) em um nó, causando um desligamento sujo do nó e forçando um despejo dos arquivos centrais ao interromper o nó. Esses comandos são úteis quando o ONTAP no nó é suspenso ou não responde a comandos como `system node shutdown` . Os arquivos de despejo de núcleo gerados são exibidos na saída do `system node coredump show` comando. O SP permanece operacional desde que a energia de entrada para o nó não seja interrompida.	Reinicie o nó com uma imagem de firmware do BIOS especificada opcionalmente (primária, backup ou atual) para se recuperar de problemas como uma imagem corrompida do dispositivo de inicialização do nó	`system reset {primary`
`backup`	`current`		`system node reset` com o `-firmware {primary` `backup`parâmetro
		`current` (nível de privilégio avançado) `system node reset`	Esta operação causa um desligamento anormal do nó. Se nenhuma imagem de firmware do BIOS for especificada, a imagem atual será usada para a reinicialização. O SP permanece operacional desde que a energia de entrada para o nó não seja interrompida.

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
Apresentar o estado da atualização automática do firmware da bateria ou ativar ou desativar a atualização automática do firmware da bateria na próxima inicialização do SP	`system battery auto_update`[`status enable`		`disable`] (nível de privilégio avançado)
		Compare a imagem atual do firmware da bateria com uma imagem de firmware especificada	`system battery verify` [`image_URL`] (nível de privilégio avançado) Se `image_URL` não for especificado, a imagem padrão do firmware da bateria será usada para comparação.
		Atualize o firmware da bateria a partir da imagem no local especificado	`system battery flash image_URL` (nível de privilégio avançado) Use este comando se o processo de atualização automática do firmware da bateria tiver falhado por algum motivo.
		Atualize o firmware do SP utilizando a imagem no local especificado	`sp update image_URL` `image_URL` não deve exceder 200 carateres.
`bmc update image_URL` `image_URL` não deve exceder 200 carateres.	`system service-processor image update`	Reinicie o SP	`sp reboot`

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
	`system service-processor reboot-sp`	Apague o conteúdo flash do NVRAM	`system nvram flash clear` (nível de privilégio avançado) Este comando não pode ser iniciado quando a alimentação do controlador está desligada (`system power off`).
		Saia da CLI do SP	`exit`

Sobre as leituras do sensor SP baseado no limiar e os valores de estado da saída do comando dos sensores do sistema

Os sensores baseados em limites fazem leituras periódicas de uma variedade de componentes do sistema. O SP compara a leitura de um sensor baseado em limites com os limites predefinidos que definem as condições de funcionamento aceitáveis de um componente.

Com base na leitura do sensor, o SP apresenta o estado do sensor para o ajudar a monitorizar a condição do componente.

Exemplos de sensores baseados em limites incluem sensores para as temperaturas do sistema, tensões, correntes e velocidades do ventilador. A lista específica de sensores baseados em limites depende da plataforma.

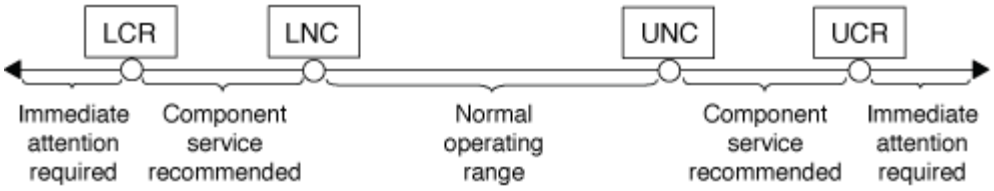
Os sensores baseados em limites têm os seguintes limites, exibidos na saída do comando SP `system sensors`:

- Crítico inferior (LCR)
- Não crítico inferior (LNC)
- Não crítico superior (UNC)
- Crítica superior (UCR)

Uma leitura do sensor entre LNC e LCR ou entre UNC e UCR significa que o componente está mostrando sinais de um problema e uma falha do sistema pode ocorrer como resultado. Portanto, você deve Planejar o serviço de componentes em breve.

Uma leitura do sensor abaixo de LCR ou acima de UCR significa que o componente está avariado e está prestes a ocorrer uma falha do sistema. Portanto, o componente requer atenção imediata.

O diagrama a seguir ilustra os intervalos de gravidade especificados pelos limites:



Você pode encontrar a leitura de um sensor baseado em limiar sob a `Current` coluna na `system sensors` saída do comando. O `system sensors get sensor_name` comando exibe detalhes adicionais para o sensor especificado. À medida que a leitura de um sensor baseado em limites cruza os limites não críticos e críticos, o sensor relata um problema de gravidade crescente. Quando a leitura excede um limite, o status do sensor na `system sensors` saída do comando muda de `ok` para `nc` (não crítico) ou `cr` (crítico) dependendo do limite excedido, e uma mensagem de evento é registrada no log de eventos SEL.

Alguns sensores baseados em limites não têm todos os quatro níveis de limiar. Para esses sensores, os limites em falta mostram `na` como seus limites na `system sensors` saída de comando, indicando que o sensor em particular não tem limite ou problema de gravidade para o determinado limite e o SP não monitora o sensor para esse limite.

Exemplo de saída de comando dos sensores do sistema

O exemplo a seguir mostra algumas das informações exibidas pelo `system sensors` comando na CLI do SP:

```
SP node1> system sensors

Sensor Name      | Current    | Unit       | Status| LCR       | LNC
| UNC       | UCR
-----------------+------------+------------+-------+-----------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
CPU1_Temp_Margin | -56.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
In_Flow_Temp     | 32.000     | degrees C  | ok    | 0.000     | 10.000
| 42.000    | 52.000
Out_Flow_Temp    | 38.000     | degrees C  | ok    | 0.000     | 10.000
| 59.000    | 68.000
CPU1_Error       | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Therm_Trip  | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Hot         | 0x0        | discrete   | 0x0180| na        | na
| na        | na
IO_Mid1_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028     | 1.048
| 1.154     | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834     | 0.844
| 1.348     | 1.368
3.3V             | 3.323      | Volts      | ok    | 3.053     | 3.116
| 3.466     | 3.546
5V               | 5.002      | Volts      | ok    | 4.368     | 4.465
| 5.490     | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678     | 1.707
| 1.892     | 1.911
…
```

Exemplo de saída do comando sensor_NAME dos sensores do sistema para um sensor baseado em limiar

O exemplo a seguir mostra o resultado da entrada `system sensors get sensor_name` na CLI do SP para o sensor 5V baseado em limiar:

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID              : 5V (0x13)
 Entity ID             : 7.97
 Sensor Type (Analog)  : Voltage
 Sensor Reading        : 5.002 (+/- 0) Volts
 Status                : ok
 Lower Non-Recoverable : na
 Lower Critical        : 4.246
 Lower Non-Critical    : 4.490
 Upper Non-Critical    : 5.490
 Upper Critical        : 5.758
 Upper Non-Recoverable : na
 Assertion Events      :
 Assertions Enabled    : lnc- lcr- ucr+
 Deassertions Enabled  : lnc- lcr- ucr+
```

Acerca dos valores de estado do sensor SP discreto da saída do comando dos sensores do sistema

Os sensores discretos não têm limites. Suas leituras, exibidas sob a `Current` coluna na saída do comando SP CLI `system sensors`, não carregam significados reais e, portanto, são ignoradas pelo SP. A `Status` coluna na `system sensors` saída do comando exibe os valores de status de sensores discretos em formato hexadecimal.

Exemplos de sensores discretos incluem sensores para a ventoinha, falha da unidade de fonte de alimentação (PSU) e falha do sistema. A lista específica de sensores discretos depende da plataforma.

Você pode usar o comando SP CLI `system sensors get sensor_name` para ajudar na interpretação dos valores de status para a maioria dos sensores discretos. Os exemplos a seguir mostram os resultados da entrada `system sensors get sensor_name` para os sensores discretos CPU0_Error e IO_SLOT1_present:

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID              : CPU0_Error (0x67)
 Entity ID             : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted       : Digital State
                         [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                         [Device Present]
```

Embora o `system sensors get sensor_name` comando exiba as informações de status para a maioria dos sensores discretos, ele não fornece informações de status para os sensores discretos System_FW_Status, System_Watchdog, PSU1_Input_Type e PSU2_Input_Type. Pode utilizar as seguintes informações para interpretar os valores de estado destes sensores.

System_FW_Status

A condição do sensor System_FW_Status aparece na forma `0xAABB` de . Pode combinar as informações de `AA` e `BB` para determinar o estado do sensor.

`AA` pode ter um dos seguintes valores:

Valores	Estado do sensor
01	Erro de firmware do sistema
02	Firmware do sistema suspenso
04	Progresso do firmware do sistema

`BB` pode ter um dos seguintes valores:

Valores	Estado do sensor
00	O software do sistema foi desligado corretamente
01	Inicialização da memória em curso
02	Inicialização do NVMEM em curso (quando o NVMEM está presente)
04	Restauração dos valores do hub do controlador de memória (MCH) (quando o NVMEM está presente)
05	O utilizador introduziu a Configuração
13	Inicializando o sistema operacional ou Loader

Valores	Estado do sensor
1F	O BIOS está a ser iniciado
20	O Loader está em execução
21	O Loader está programando o firmware principal do BIOS. Não deve desligar o sistema.
22	O Loader está programando o firmware alternativo do BIOS. Não deve desligar o sistema.
2F	O ONTAP está em execução
60	O SP desligou o sistema
61	O SP ligou o sistema
62	O SP redefiniu o sistema
63	Ciclo de alimentação do SP watchdog
64	Reinicialização a frio do SP watchdog

Por exemplo, o estado 0x042F do sensor System_FW_Status significa "progresso do firmware do sistema (04), ONTAP está em execução (2F)".

System_Watchdog

O sensor System_Watchdog pode ter uma das seguintes condições:

- **0x0080**

  O estado deste sensor não mudou

Valores	Estado do sensor
0x0081	Interrupção do temporizador
0x0180	O temporizador expirou
0x0280	Reinicialização total
0x0480	Desligar
0x0880	Ciclo de alimentação

Por exemplo, o estado 0x0880 do sensor System_Watchdog significa que ocorre um tempo limite de monitorização e provoca um ciclo de alimentação do sistema.

PSU1_Input_Type e PSU2_Input_Type

Para fontes de alimentação de corrente contínua (DC), os sensores PSU1_Input_Type e PSU2_Input_Type não se aplicam. Para fontes de alimentação de corrente alternada (AC), o estado dos sensores pode ter um dos seguintes valores:

Valores	Estado do sensor
0x01 xx	220V tipo de PSU
0x02 xx	110V tipo de PSU

Por exemplo, o estado 0x0280 do sensor PSU1_Input_Type significa que o sensor informa que o tipo de PSU é 110V.

Comandos para gerenciar o SP a partir do ONTAP

O ONTAP fornece comandos para gerenciar o SP, incluindo a configuração de rede SP, a imagem de firmware do SP, o acesso SSH ao SP e a administração geral do SP.

Comandos para gerenciar a configuração de rede SP

Se você quiser…	Execute este comando ONTAP…
Ative a configuração automática de rede SP para o SP usar a família de endereços IPv4 ou IPv6 da sub-rede especificada	`system service-processor network auto-configuration enable`
Desative a configuração automática de rede SP para a família de endereços IPv4 ou IPv6 da sub-rede especificada para o SP	`system service-processor network auto-configuration disable`
Apresentar a configuração automática da rede SP	`system service-processor network auto-configuration show`

Se você quiser…	Execute este comando ONTAP…
Configure manualmente a rede SP para um nó, incluindo o seguinte: • A família de endereços IP (IPv4 ou IPv6) • Se a interface de rede da família de endereços IP especificada deve ser ativada • Se estiver a utilizar IPv4, utilize a configuração de rede a partir do servidor DHCP ou o endereço de rede especificado • O endereço IP público do SP • A máscara de rede para o SP (se utilizar IPv4) • O tamanho do prefixo da rede da máscara de sub-rede para o SP (se estiver usando IPv6) • O endereço IP do gateway para o SP	`system service-processor network modify`
Exiba a configuração de rede SP, incluindo o seguinte: • A família de endereços configurada (IPv4 ou IPv6) e se está ativada • O tipo de dispositivo de gerenciamento remoto • O estado atual do SP e o estado da ligação • Configuração de rede, como endereço IP, endereço MAC, máscara de rede, tamanho do prefixo da máscara de sub-rede, endereço IP atribuído pelo roteador, endereço IP local do link e endereço IP do gateway • A hora em que o SP foi atualizado pela última vez • O nome da sub-rede utilizada para a configuração automática do SP • Se o endereço IP atribuído ao router IPv6 está ativado • Estado da configuração da rede SP • Motivo da falha de configuração da rede SP	`system service-processor network show` A exibição de detalhes completos da rede SP requer o `-instance` parâmetro.
Modifique a configuração do serviço API do SP, incluindo o seguinte: • Alterar a porta usada pelo serviço de API do SP • Ativar ou desativar o serviço de API SP	`system service-processor api-service modify` (nível de privilégio avançado)

Se você quiser…	Execute este comando ONTAP…
Exibir a configuração do serviço da API do SP	`system service-processor api-service show` (nível de privilégio avançado)
Renove os certificados SSL e SSH usados pelo serviço API SP para comunicação interna	• Para o ONTAP 9.5 ou posterior: `system service-processor api-service renew-internal-certificates` • Para o ONTAP 9.4 ou anterior: `system service-processor api-service renew-certificates` (nível de privilégio avançado)

Comandos para gerenciar a imagem de firmware do SP

Se você quiser…	Execute este comando ONTAP…
Exiba os detalhes da imagem de firmware do SP atualmente instalada, incluindo o seguinte: • O tipo de dispositivo de gerenciamento remoto • A imagem (principal ou backup) da qual o SP é inicializado, seu status e versão do firmware • Se a atualização automática do firmware está ativada e o estado da última atualização	`system service-processor image show` O `-is-current` parâmetro indica a imagem (primária ou de cópia de segurança) da qual o SP está atualmente inicializado, não se a versão do firmware instalada for a mais atual.
Ative ou desative a atualização automática de firmware do SP	`system service-processor image modify` Por padrão, o firmware do SP é atualizado automaticamente com a atualização do ONTAP ou quando uma nova versão do firmware do SP é baixada manualmente. Desativar a atualização automática não é recomendado porque isso pode resultar em combinações subótimas ou não qualificadas entre a imagem ONTAP e a imagem de firmware SP.

Se você quiser…	Execute este comando ONTAP…
Transfira manualmente uma imagem de firmware SP num nó	`system node image get` Antes de executar os `system node image` comandos, você deve definir o nível de privilégio como avançado (`set -privilege advanced`), inserindo **y** quando solicitado a continuar. A imagem de firmware do SP é fornecida com o ONTAP. Não é necessário baixar o firmware do SP manualmente, a menos que você queira usar uma versão de firmware do SP diferente da fornecida com o ONTAP.
Exiba o status da última atualização de firmware do SP acionada pelo ONTAP, incluindo as seguintes informações: • A hora de início e fim da atualização de firmware mais recente do SP • Se uma atualização está em andamento e a porcentagem que está concluída	`system service-processor image update-progress show`

Comandos para gerenciar o acesso SSH ao SP

Se você quiser…	Execute este comando ONTAP…
Conceda acesso SP apenas aos endereços IP especificados	`system service-processor ssh add-allowed-addresses`
Bloquear o acesso aos endereços IP especificados ao SP	`system service-processor ssh remove-allowed-addresses`
Exiba os endereços IP que podem acessar o SP	`system service-processor ssh show`

Comandos para administração geral do SP

Se você quiser…	Execute este comando ONTAP…
Exibir informações gerais do SP, incluindo o seguinte: • O tipo de dispositivo de gerenciamento remoto • O estado atual do SP • Se a rede SP está configurada • Informações de rede, como o endereço IP público e o endereço MAC • A versão do firmware do SP e a versão da interface de gestão inteligente da plataforma (IPMI) • Se a atualização automática do firmware do SP está ativada	`system service-processor show` A exibição de informações completas do SP requer o `-instance` parâmetro.
Reinicie o SP em um nó	`system service-processor reboot-sp`
Gere e envie uma mensagem do AutoSupport que inclua os arquivos de log do SP coletados de um nó especificado	`system node autosupport invoke-splog`
Exiba o mapa de alocação dos arquivos de log do SP coletados no cluster, incluindo os números de sequência dos arquivos de log do SP que residem em cada nó de coleta	`system service-processor log show-allocations`

Informações relacionadas

"Referência do comando ONTAP"

Comandos ONTAP para gerenciamento de BMC

Esses comandos ONTAP são suportados no controlador de gerenciamento da placa base (BMC).

O BMC usa alguns dos mesmos comandos que o processador de serviço (SP). Os seguintes comandos SP são suportados no BMC.

Se você quiser…	Use este comando
Apresentar as informações do BMC	**`system service-processor show`**
Apresentar/modificar a configuração da rede BMC	**`system service-processor network show/modify`**
Reinicie o BMC	**`system service-processor reboot-sp`**

Se você quiser…	Use este comando
Apresentar/modificar os detalhes da imagem de firmware do BMC instalada atualmente	**system service-processor image show/modify**
Atualize o firmware do BMC	**system service-processor image update**
Apresentar o estado da atualização de firmware do BMC mais recente	**system service-processor image update-progress show**
Ative a configuração automática de rede para o BMC usar um endereço IPv4 ou IPv6 na sub-rede especificada	**system service-processor network auto-configuration enable**
Desative a configuração automática de rede para um endereço IPv4 ou IPv6 na sub-rede especificada para o BMC	**system service-processor network auto-configuration disable**
Apresentar a configuração automática da rede BMC	**system service-processor network auto-configuration show**

Para comandos que não são suportados pelo firmware do BMC, a seguinte mensagem de erro é retornada.

```
::> Error: Command not supported on this platform.
```

Comandos CLI do BMC

Você pode fazer login no BMC usando SSH. Os seguintes comandos são suportados a partir da linha de comando BMC.

Comando	Função
sistema	Exibir uma lista de todos os comandos.
consola do sistema	Ligue à consola do sistema. `Ctrl+D`Utilize para sair da sessão.
núcleo do sistema	Descarregue o núcleo do sistema e reinicie.
ciclo de alimentação do sistema	Desligue o sistema e, em seguida, ligue-o.
desligar o sistema	Desligue o sistema.
ligar o sistema	Ligue o sistema.

Comando	Função
estado de alimentação do sistema	Estado de alimentação do sistema de impressão.
reposição do sistema	Reinicie o sistema.
registo do sistema	Imprimir registos da consola do sistema
apresentação da fru do sistema [id]	Despejar todas/informações da unidade substituível em campo (FRU) selecionada.

Gerenciar o tempo do cluster (somente administradores de cluster)

Podem ocorrer problemas quando o tempo do cluster é impreciso. Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

O NTP está sempre ativado. No entanto, a configuração ainda é necessária para que o cluster sincronize com uma fonte de tempo externa. O ONTAP permite gerenciar a configuração NTP do cluster das seguintes maneiras:

- Pode associar um máximo de 10 servidores NTP externos ao cluster (`cluster time-service ntp server create`).
  - Para redundância e qualidade do serviço de tempo, você deve associar pelo menos três servidores NTP externos ao cluster.
  - Você pode especificar um servidor NTP usando seu endereço IPv4 ou IPv6 ou nome de host totalmente qualificado.
  - Pode especificar manualmente a versão NTP (v3 ou v4) a utilizar.

    Por padrão, o ONTAP seleciona automaticamente a versão NTP que é suportada para um determinado servidor NTP externo.

  Se a versão NTP especificada não for suportada para o servidor NTP, a troca de tempo não poderá ocorrer.
  - No nível de privilégio avançado, você pode especificar um servidor NTP externo que está associado ao cluster para ser a principal fonte de tempo para corrigir e ajustar a hora do cluster.
- Pode visualizar os servidores NTP associados ao cluster (`cluster time-service ntp server show`).
- Pode modificar a configuração NTP do cluster (`cluster time-service ntp server modify`).
- Você pode desassociar o cluster de um servidor NTP externo (`cluster time-service ntp server delete`).
- No nível de privilégio avançado, pode repor a configuração limpando a associação de todos os servidores NTP externos com o cluster (`cluster time-service ntp server reset`).

Um nó que se junta a um cluster adota automaticamente a configuração NTP do cluster.

Além de usar o NTP, o ONTAP também permite gerenciar manualmente o tempo do cluster. Esse recurso é útil quando você precisa corrigir o tempo errado (por exemplo, o tempo de um nó ficou significativamente incorreto após uma reinicialização). Nesse caso, você pode especificar um tempo aproximado para o cluster até que o NTP possa sincronizar com um servidor de hora externo. O tempo definido manualmente entra em vigor em todos os nós do cluster.

Você pode gerenciar manualmente o tempo do cluster das seguintes maneiras:

- Pode definir ou modificar o fuso horário, a data e a hora no cluster (`cluster date modify`).
- Pode apresentar as definições atuais de fuso horário, data e hora do cluster (`cluster date show`).

> As programações de trabalhos não se ajustam às alterações manuais de data e hora do cluster. Esses trabalhos são programados para serem executados com base na hora atual do cluster quando o trabalho foi criado ou quando o trabalho foi executado mais recentemente. Portanto, se você alterar manualmente a data ou a hora do cluster, use os `job show` comandos e `job history show` para verificar se todos os trabalhos agendados estão na fila e concluídos de acordo com seus requisitos.

Comandos para gerenciar o tempo do cluster

Você usa os `cluster time-service ntp server` comandos para gerenciar os servidores NTP para o cluster. Você usa os `cluster date` comandos para gerenciar o tempo do cluster manualmente.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Os comandos a seguir permitem gerenciar os servidores NTP para o cluster:

Se você quiser…	Use este comando…
Associe o cluster a um servidor NTP externo sem autenticação simétrica	`cluster time-service ntp server create -server server_name`
Associe o cluster a um servidor NTP externo com autenticação simétrica Artigo disponível no ONTAP 9.5 ou posterior	`cluster time-service ntp server create -server server_ip_address -key-id key_id` O `key_id` deve se referir a uma chave compartilhada existente configurada com "chave ntp de serviço de tempo do cluster'.
Ativar autenticação simétrica para um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID de chave necessária. Disponível no ONTAP 9.5 ou posterior	`cluster time-service ntp server modify -server server_name -key-id key_id`

Se você quiser…	Use este comando…
Desativar a autenticação simétrica	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`
Configurar uma chave NTP partilhada	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` As chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP
Exibir informações sobre os servidores NTP associados ao cluster	`cluster time-service ntp server show`
Modifique a configuração de um servidor NTP externo associado ao cluster	`cluster time-service ntp server modify`
Dissociar um servidor NTP do cluster	`cluster time-service ntp server delete`
Redefina a configuração limpando a associação de todos os servidores NTP externos com o cluster	`cluster time-service ntp server reset` Este comando requer o nível de privilégio avançado.

Os comandos a seguir permitem gerenciar o tempo do cluster manualmente:

Se você quiser…	Use este comando…
Defina ou modifique o fuso horário, a data e a hora	`cluster date modify`
Exiba as configurações de fuso horário, data e hora do cluster	`cluster date show`

Informações relacionadas

"Referência do comando ONTAP"

Gerencie o banner e o MOTD

Gerencie o banner e a visão geral do MOTD

O ONTAP permite configurar um banner de login ou uma mensagem do dia (MOTD) para comunicar informações administrativas aos usuários da CLI do cluster ou máquina virtual de armazenamento (SVM).

Um banner é exibido em uma sessão de console (apenas para acesso ao cluster) ou uma sessão SSH (para acesso ao cluster ou SVM) antes que um usuário seja solicitado a autenticação, como uma senha. Por exemplo, você pode usar o banner para exibir uma mensagem de aviso como a seguinte para alguém que tenta fazer login no sistema:

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

Um MOTD é exibido em uma sessão de console (apenas para acesso de cluster) ou uma sessão SSH (para acesso de cluster ou SVM) depois que um usuário é autenticado, mas antes que o prompt de clustershell seja exibido. Por exemplo, você pode usar o MOTD para exibir uma mensagem de boas-vindas ou informativa, como a seguinte, que somente usuários autenticados verão:

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

Você pode criar ou modificar o conteúdo do banner ou MOTD usando o `security login banner modify` comando ou `security login motd modify`, respetivamente, das seguintes maneiras:

- Você pode usar a CLI interativamente ou não interativamente para especificar o texto a ser usado para o banner ou MOTD.

  O modo interativo, iniciado quando o comando é usado sem o `-message` parâmetro ou `-uri`, permite que você use novas linhas (também conhecidas como final de linhas) na mensagem.

  O modo não interativo, que usa o `-message` parâmetro para especificar a cadeia de carateres da mensagem, não suporta novas linhas.

- Você pode fazer upload de conteúdo de um local FTP ou HTTP para usar para o banner ou MOTD.
- Pode configurar o MOTD para apresentar conteúdo dinâmico.

  Exemplos do que você pode configurar o MOTD para exibir dinamicamente incluem o seguinte:

  - Nome do cluster, nome do nó ou nome do SVM
  - Data e hora do cluster
  - Nome do utilizador que inicia sessão
  - Último login para o usuário em qualquer nó no cluster
  - Nome do dispositivo de início de sessão ou endereço IP

- Nome do sistema operacional
- Versão de versão do software
- String de versão de cluster eficaz a `security login motd modify` página man descreve as sequências de escape que você pode usar para ativar o MOTD para exibir conteúdo gerado dinamicamente.

O banner não suporta conteúdo dinâmico.

Você pode gerenciar o banner e o MOTD no nível do cluster ou SVM:

- Os seguintes fatos se aplicam ao banner:
  - O banner configurado para o cluster também é usado para todos os SVMs que não têm uma mensagem de banner definida.
  - É possível configurar um banner no nível da SVM para cada SVM.

    Se um banner no nível do cluster tiver sido configurado, ele será substituído pelo banner no nível da SVM para determinado SVM.
- Os seguintes factos aplicam-se ao MOTD:
  - Por padrão, o MOTD configurado para o cluster também é ativado para todos os SVMs.
  - Além disso, é possível configurar um MOTD no nível da SVM para cada SVM.

    Nesse caso, os usuários que fizerem login no SVM verão dois MOTDs, um definido no nível do cluster e o outro no nível SVM.
  - O MOTD no nível do cluster pode ser ativado ou desativado por SVM pelo administrador do cluster.

    Se o administrador do cluster desativar o MOTD em nível de cluster para um SVM, um usuário que faz login no SVM não verá o MOTD em nível de cluster.

Crie um banner

Você pode criar um banner para exibir uma mensagem para alguém que tente acessar o cluster ou SVM. O banner é exibido em uma sessão de console (apenas para acesso ao cluster) ou em uma sessão SSH (para acesso ao cluster ou SVM) antes que um usuário seja solicitado a autenticação.

Passos

1. Use o `security login banner modify` comando para criar um banner para o cluster ou SVM:

Se você quiser…	Então…
Especifique uma mensagem que seja uma única linha	Utilize o `-messagetext` parâmetro " " para especificar o texto.
Inclua novas linhas (também conhecidas como fim de linhas) na mensagem	Use o comando sem o `-message` parâmetro ou `-uri` para iniciar o modo interativo para editar o banner.

Se você quiser…	Então…
Faça upload de conteúdo de um local para usar para o banner	Use o `-uri` parâmetro para especificar a localização FTP ou HTTP do conteúdo.

O tamanho máximo para um banner é de 2.048 bytes, incluindo novas linhas.

Um banner criado usando o `-uri` parâmetro é estático. Não é atualizado automaticamente para refletir as alterações subsequentes do conteúdo fonte.

O banner criado para o cluster também é exibido para todos os SVMs que não têm um banner existente. Qualquer banner criado posteriormente para um SVM substitui o banner no nível do cluster desse SVM. Especificar o `-message` parâmetro com um hífen entre aspas duplas (`"-"`) para o SVM redefine o SVM para usar o banner no nível do cluster.

2. Verifique se o banner foi criado exibindo-o com o `security login banner show` comando.

   Especificar o `-message` parâmetro com uma string vazia (`""`) exibe banners que não têm conteúdo.

   Especificar o `-message` parâmetro com `"-"` exibe todos os SVMs (admin ou dados) que não têm um banner configurado.

Exemplos de criação de banners

O exemplo a seguir usa o modo não interativo para criar um banner para o cluster "'cluster1"":

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

O exemplo a seguir usa o modo interativo para criar um banner para o "VM1" SVM:

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

O exemplo a seguir exibe os banners que foram criados:

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

Informações relacionadas

Gerenciar o banner

Gerenciar o banner

É possível gerenciar o banner no nível do cluster ou SVM. O banner configurado para o cluster também é usado para todos os SVMs que não têm uma mensagem de banner definida. Um banner criado posteriormente para um SVM substitui o banner do cluster para esse SVM.

Opções

- Gerencie o banner no nível do cluster:

Se você quiser…	Então…
Crie um banner para exibir todas as sessões de login da CLI	Definir um banner no nível do cluster: `*security login banner modify -vserver *cluster_name* { [-message "text"]
[*-uri ftp_or_http_addr*] }*`	Remova o banner para todos os logins (cluster e SVM)
Defina o banner para uma string vazia (""): **`security login banner modify -vserver * -message ""`**	Substituir um banner criado por um administrador SVM

Se você quiser…	Então…
Modifique a mensagem de banner SVM: `*security login banner modify -vserver *svm_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] }*`

- Gerencie o banner no nível da SVM:

  Não é necessário especificar `-vserver *svm_name*` no contexto SVM.

Se você quiser…	Então…
Substitua o banner fornecido pelo administrador do cluster por um banner diferente para o SVM	Crie um banner para o SVM: `*security login banner modify -vserver *svm_name* { [-message "text"]
[-uri ftp_or_http_addr] }*`	Suprimir o banner fornecido pelo administrador do cluster para que nenhum banner seja exibido para o SVM
Defina o banner SVM para uma cadeia vazia para o SVM: **`security login banner modify -vserver *svm_name* -message ""`**	Use o banner no nível do cluster quando o SVM usar um banner no nível da SVM

Crie um MOTD

Você pode criar uma mensagem do dia (MOTD) para comunicar informações a usuários CLI autenticados. O MOTD é exibido em uma sessão de console (somente para acesso ao cluster) ou em uma sessão SSH (para acesso ao cluster ou SVM) depois que um usuário é autenticado, mas antes que o prompt do clustershell seja exibido.

Passos

1. Use o `security login motd modify` comando para criar um MOTD para o cluster ou SVM:

Se você quiser…	Então…
Especifique uma mensagem que seja uma única linha	Utilize o `-messagetext` parâmetro " " para especificar o texto.
Incluir novas linhas (também conhecido como fim de linhas)	Use o comando sem o `-message` parâmetro ou `-uri` para iniciar o modo interativo para editar o MOTD.

Se você quiser…	Então…
Faça upload de conteúdo de um local para usar para o MOTD	Use o `-uri` parâmetro para especificar a localização FTP ou HTTP do conteúdo.

O tamanho máximo para um MOTD é de 2.048 bytes, incluindo novas linhas.

A `security login motd modify` página man descreve as sequências de escape que você pode usar para ativar o MOTD para exibir conteúdo gerado dinamicamente.

Um MOTD criado usando o `-uri` parâmetro é estático. Não é atualizado automaticamente para refletir as alterações subsequentes do conteúdo fonte.

Um MOTD criado para o cluster também é exibido para todos os logins SVM por padrão, juntamente com um MOTD no nível SVM que você pode criar separadamente para um determinado SVM. Definir o `-is -cluster-message-enabled` parâmetro como `false` para um SVM impede que o MOTD no nível do cluster seja exibido para esse SVM.

2. Verifique se o MOTD foi criado exibindo-o com o `security login motd show` comando.

   Especificando o `-message` parâmetro com uma string vazia (`""`) exibe MOTDs que não estão configurados ou não têm conteúdo.

   Consulte a "segurança login motd modificar" página man do comando para obter uma lista de parâmetros a serem usados para permitir que o MOTD exiba conteúdo gerado dinamicamente. Certifique-se de verificar a página de manual específica para a sua versão do ONTAP.

Exemplos de criação de MOTDs

O exemplo a seguir usa o modo não interativo para criar um MOTD para o cluster ""cluster1"":

```
cluster1::> security login motd modify -message "Greetings!"
```

O exemplo a seguir usa o modo interativo para criar um MOTD para o SVM "VM1" que usa sequências de escape para exibir conteúdo gerado dinamicamente:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

O exemplo a seguir exibe os MOTDs que foram criados:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

Gerencie o MOTD no ONTAP

É possível gerenciar a mensagem do dia (MOTD) no nível do cluster ou SVM. Por padrão, o MOTD configurado para o cluster também é ativado para todos os SVMs. Além disso, é possível configurar um MOTD no nível da SVM para cada SVM. O MOTD no nível do cluster pode ser ativado ou desativado para cada SVM pelo administrador do cluster.

Saiba mais sobre o "sequências de fuga" que pode ser usado para gerar conteúdo dinamicamente para o MOTD na referência de comando ONTAP.

Opções

- Gerencie o MOTD no nível do cluster:

Se você quiser…	Então…
Crie um MOTD para todos os logins quando não houver MOTD existente	Definir um MOTD de nível de cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Altere o MOTD para todos os logins quando nenhum MOTDs no nível SVM estiver configurado

Se você quiser…	Então…
Modifique o MOTD no nível do cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"] }	[-uri ftp_or_http_addr] }*`
Remova o MOTD para todos os logins quando nenhum MOTDs de nível SVM estiver configurado	Defina o MOTD de nível de cluster para uma cadeia vazia (`""`): **`security login motd modify -vserver *cluster_name* -message ""`**
Peça a cada SVM que exiba o MOTD no nível do cluster em vez de usar o MOTD no nível da SVM	Defina um MOTD de nível de cluster e, em seguida, defina todos os MOTDs de nível SVM para uma cadeia vazia com o MOTD de nível de cluster ativado: a. `*security login motd modify -vserver *cluster_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*` .. **`security login motd modify { -vserver !"*cluster_name*" } -message "" -is -cluster-message-enabled true`**	Tenha um MOTD exibido apenas para SVMs selecionadas e não use nenhum MOTD no nível do cluster
Defina o MOTD de nível de cluster para uma cadeia vazia e, em seguida, defina MOTDs de nível SVM para SVMs selecionadas: a. **`security login motd modify -vserver *cluster_name* -message ""`** b. `*security login motd modify -vserver *svm_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] }*` + Você pode repetir esta etapa para cada SVM conforme necessário.
Use o mesmo MOTD no nível da SVM para todos os SVMs (dados e administradores)	Defina o cluster e todos os SVMs para usar o mesmo MOTD: `*security login motd modify *-vserver* * { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*` [NOTE] ==== Se você usar o modo interativo, a CLI solicitará que você insira o MOTD individualmente para o cluster e cada SVM. Você pode colar o mesmo MOTD em cada instância quando for solicitado. ====	Tenha um MOTD de nível de cluster disponível opcionalmente para todos os SVMs, mas não queira que o MOTD seja exibido para logins de cluster

Se você quiser…	Então…
Defina um MOTD no nível do cluster, mas desative sua exibição para o cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] } -is-cluster-message-enabled false*`
Remova todos os MOTDs nos níveis de cluster e SVM quando apenas alguns SVMs tiverem MOTDs no nível do cluster e SVM	Defina o cluster e todos os SVMs para usar uma cadeia vazia para o MOTD: **`security login motd modify -vserver * -message ""`**
Modifique o MOTD apenas para os SVMs que têm uma cadeia de carateres não vazia, quando outros SVMs usam uma cadeia vazia e quando um MOTD diferente é usado no nível do cluster	Use consultas estendidas para modificar o MOTD seletivamente: `*security login motd modify { -vserver !"*cluster_name*" -message !"" } { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Exibir todos os MOTDs que contêm texto específico (por exemplo, "'janeiro"" seguido de "'2015"") em qualquer lugar em uma mensagem única ou multilinha, mesmo que o texto seja dividido em linhas diferentes
Use uma consulta para exibir MOTDs: **`security login motd show -message *"January"*"2015"*`**	Crie interativamente um MOTD que inclua novas linhas múltiplas e consecutivas (também conhecidas como fim de linhas, ou EOLS)

- Gerencie o MOTD no nível SVM:

  Não é necessário especificar `-vserver *svm_name*` no contexto SVM.

Se você quiser…	Então…
Use um MOTD no nível da SVM diferente, quando o SVM já tiver um MOTD no nível da SVM	Modifique o MOTD no nível da SVM: `*security login motd modify -vserver *svm_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Use apenas o MOTD no nível do cluster para SVM, quando o SVM já tiver um MOTD no nível do SVM

Se você quiser…	Então…
Defina o SVM-level MOTD para uma cadeia vazia e, em seguida, faça com que o administrador de cluster ative o cluster-level MOTD para o SVM: a. **`security login motd modify -vserver *svm_name* -message ""`** b. (Para o administrador do cluster) **`security login motd modify -vserver *svm_name* -is-cluster-message-enabled true`**	Não é possível que o SVM exiba nenhum MOTD quando os MOTDs de nível de cluster e SVM forem exibidos atualmente para o SVM

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Gerenciar trabalhos e agendar

Os trabalhos são colocados em uma fila de trabalhos e executados em segundo plano quando os recursos estão disponíveis. Se uma tarefa estiver consumindo muitos recursos de cluster, você pode pará-la ou pausar até que haja menos demanda no cluster. Também pode monitorizar e reiniciar trabalhos.

Categorias de trabalho

Existem três categorias de trabalhos que você pode gerenciar: Afiliados ao servidor, afiliados a cluster e privados.

Um trabalho pode estar em qualquer uma das seguintes categorias:

- **Empregos afiliados ao servidor**

  Esses trabalhos são enfileirados pela estrutura de gerenciamento para um nó específico a ser executado.

- **Empregos afiliados a cluster**

  Esses trabalhos são enfileirados pela estrutura de gerenciamento para qualquer nó no cluster a ser executado.

- **Empregos privados**

  Essas tarefas são específicas para um nó e não usam o banco de dados replicado (RDB) ou qualquer outro mecanismo de cluster. Os comandos que gerem trabalhos privados requerem o nível de privilégio avançado ou superior.

Comandos para gerir trabalhos

Quando você insere um comando que invoca uma tarefa, normalmente, o comando informa que a tarefa foi enfileirada e retorna ao prompt de comando CLI. No entanto, alguns comandos reportam o progresso da tarefa e não retornam ao prompt de comando da CLI até que a tarefa seja concluída. Nesses casos, você pode pressionar Ctrl-C para mover o trabalho para o fundo.

Se você quiser…	Use este comando…
Exibir informações sobre todos os trabalhos	`job show`
Exibir informações sobre trabalhos por nó	`job show bynode`
Exibir informações sobre trabalhos afiliados ao cluster	`job show-cluster`
Exibir informações sobre os trabalhos concluídos	`job show-completed`
Apresentar informações sobre o histórico de trabalhos	`job history show` São armazenados até 25.000 registos de trabalho para cada nó no cluster. Consequentemente, tentar exibir o histórico completo do trabalho pode levar muito tempo. Para evitar tempos de espera potencialmente longos, você deve exibir tarefas por nó, máquina virtual de armazenamento (SVM) ou ID de Registro.
Apresentar a lista de trabalhos privados	`job private show` (nível de privilégio avançado)
Exibir informações sobre trabalhos privados concluídos	`job private show-completed` (nível de privilégio avançado)
Exibir informações sobre o estado de inicialização para gerentes de tarefas	`job initstate show` (nível de privilégio avançado)
Monitorize o progresso de um trabalho	`job watch-progress`
Monitore o progresso de um trabalho privado	`job private watch-progress` (nível de privilégio avançado)
Pausar um trabalho	`job pause`
Pausar um trabalho privado	`job private pause` (nível de privilégio avançado)
Retomar um trabalho em pausa	`job resume`
Retomar um trabalho privado em pausa	`job private resume` (nível de privilégio avançado)
Parar um trabalho	`job stop`
Parar um trabalho privado	`job private stop` (nível de privilégio avançado)

Se você quiser…	Use este comando…
Eliminar um trabalho	`job delete`
Eliminar um trabalho privado	`job private delete` (nível de privilégio avançado)
Desassocie uma tarefa afiliada ao cluster a um nó não disponível que o possua, para que outro nó possa assumir a propriedade dessa tarefa	`job unclaim` (nível de privilégio avançado)

Você pode usar o `event log show` comando para determinar o resultado de uma tarefa concluída.

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerir agendas de trabalhos

Muitas tarefas - por exemplo, cópias Snapshot de volume - podem ser configuradas para serem executadas em programações especificadas.os horários que são executados em momentos específicos são chamados de programações *cron* (semelhantes às programações UNIX `cron`). As programações que são executadas em intervalos são chamadas *interval* programações. Utilize os `job schedule` comandos para gerir agendas de trabalhos.

As programações de trabalhos não se ajustam às alterações manuais da data e hora do cluster. Esses trabalhos são programados para serem executados com base na hora atual do cluster quando o trabalho foi criado ou quando o trabalho foi executado mais recentemente. Portanto, se você alterar manualmente a data ou a hora do cluster, use os `job show` comandos e `job history show` para verificar se todos os trabalhos agendados estão na fila e concluídos de acordo com seus requisitos.

Se o cluster fizer parte de uma configuração do MetroCluster, as programações de tarefas em ambos os clusters devem ser idênticas. Portanto, se você criar, modificar ou excluir um agendamento de trabalhos, deverá executar a mesma operação no cluster remoto.

Se você quiser…	Use este comando…
Exibir informações sobre todas as programações	`job schedule show`
Exibir a lista de trabalhos por agendamento	`job schedule show-jobs`
Exibir informações sobre cronogramas do cron	`job schedule cron show`
Exibir informações sobre programações de intervalos	`job schedule interval show`

Se você quiser…	Use este comando…
Crie um cronograma cron	`job schedule cron create` A partir do ONTAP 9.10,1, você pode incluir o SVM para sua agenda de trabalho.
Crie um agendamento de intervalos	`job schedule interval create` É necessário especificar pelo menos um dos seguintes parâmetros: `-days`, `-hours`, `-minutes`, `-seconds` Ou .
Modifique um cronograma do cron	`job schedule cron modify`
Modificar um agendamento de intervalos	`job schedule interval modify`
Eliminar uma agenda	`job schedule delete`
Exclua um cronograma do cron	`job schedule cron delete`
Eliminar um agendamento de intervalos	`job schedule interval delete`

Informações relacionadas

"Referência do comando ONTAP"

Fazer backup e restaurar configurações de cluster (somente administradores de cluster)

Quais são os arquivos de backup de configuração

Os arquivos de backup de configuração são arquivos de arquivo (.7z) que contêm informações para todas as opções configuráveis que são necessárias para o cluster e os nós dentro dele, para operar corretamente.

Esses arquivos armazenam a configuração local de cada nó, além da configuração replicada em todo o cluster. Você usa arquivos de backup de configuração para fazer backup e restaurar a configuração do cluster.

Existem dois tipos de arquivos de backup de configuração:

- * Ficheiro de cópia de segurança da configuração do nó*

  Cada nó íntegro no cluster inclui um arquivo de backup de configuração de nós, que contém todas as informações de configuração e metadados necessários para que o nó opere de forma saudável no cluster.

- **Ficheiro de cópia de segurança de configuração de cluster**

  Esses arquivos incluem um arquivo de todos os arquivos de backup de configuração de nó no cluster, além das informações replicadas de configuração de cluster (o banco de dados replicado ou arquivo

RDB). Os arquivos de backup de configuração de cluster permitem restaurar a configuração de todo o cluster ou de qualquer nó no cluster. As programações de backup de configuração de cluster criam esses arquivos automaticamente e os armazenam em vários nós no cluster.

> Os ficheiros de cópia de segurança de configuração contêm apenas informações de configuração. Eles não incluem nenhum dado de usuário. Para obter informações sobre como restaurar dados do usuário, "Proteção de dados"consulte .

Como o backup automático das configurações de nó e cluster é feito automaticamente

Três programações separadas criam automaticamente arquivos de backup de configuração de cluster e nó e replicam-os entre os nós do cluster.

Os arquivos de backup de configuração são criados automaticamente de acordo com as seguintes programações:

- A cada 8 horas
- Diariamente
- Semanalmente

Em cada um desses momentos, um arquivo de backup de configuração de nós é criado em cada nó íntegro no cluster. Todos esses arquivos de backup de configuração de nó são coletados em um único arquivo de backup de configuração de cluster, juntamente com a configuração de cluster replicada e salvos em um ou mais nós no cluster.

Comandos para gerenciar programações de backup de configuração

Você pode usar os `system configuration backup settings` comandos para gerenciar programações de backup de configuração.

Esses comandos estão disponíveis no nível avançado de privilégio.

Se você quiser…	Use este comando…
Altere as configurações de um agendamento de backup de configuração: • Especifique um URL remoto (HTTP, HTTPS, FTP, FTPS ou TFTP) onde os arquivos de backup de configuração serão carregados além dos locais padrão no cluster • Especifique um nome de usuário a ser usado para fazer login no URL remoto • Defina o número de backups a serem mantidos para cada agendamento de backup de configuração	`system configuration backup settings modify` Quando utilizar HTTPS na URL remota, utilize a `-validate-certification` opção para ativar ou desativar a validação de certificados digitais. A validação do certificado está desativada por predefinição. O servidor da Web para o qual você está fazendo o upload do arquivo de backup de configuração deve ter as operações de COLOCAÇÃO ativadas para HTTP e POST ativadas para HTTPS. Para obter mais informações, consulte a documentação do servidor Web.
Defina a senha a ser usada para fazer login no URL remoto	`system configuration backup settings set-password`
Ver as definições do agendamento da cópia de segurança da configuração	`system configuration backup settings show` Você define o `-instance` parâmetro para exibir o nome de usuário e o número de backups a serem mantidos para cada agendamento.

Comandos para gerenciar arquivos de backup de configuração

Você usa os `system configuration backup` comandos para gerenciar arquivos de backup de configuração de cluster e nó.

Esses comandos estão disponíveis no nível avançado de privilégio.

Se você quiser…	Use este comando…
Crie um novo arquivo de backup de configuração de nó ou cluster	`system configuration backup create`
Copie um arquivo de backup de configuração de um nó para outro nó no cluster	`system configuration backup copy`

Se você quiser…	Use este comando…
Carregar um arquivo de backup de configuração de um nó no cluster para um URL remoto (FTP, HTTP, HTTPS, TFTP ou FTPS)	`system configuration backup upload` Quando utilizar HTTPS na URL remota, utilize a `-validate-certification` opção para ativar ou desativar a validação de certificados digitais. A validação do certificado está desativada por predefinição. O servidor da Web para o qual você está fazendo o upload do arquivo de backup de configuração deve ter as operações de COLOCAÇÃO ativadas para HTTP e POST ativadas para HTTPS. Alguns servidores da Web podem exigir a instalação de um módulo adicional. Para obter mais informações, consulte a documentação do servidor Web. Os formatos de URL suportados variam de acordo com a versão do ONTAP. Saiba mais sobre os comandos de configuração do sistema no ""Referência do comando ONTAP".
Faça o download de um arquivo de backup de configuração de um URL remoto para um nó no cluster e, se especificado, valide o certificado digital	`system configuration backup download` Quando utilizar HTTPS na URL remota, utilize a `-validate-certification` opção para ativar ou desativar a validação de certificados digitais. A validação do certificado está desativada por predefinição.
Renomeie um arquivo de backup de configuração em um nó no cluster	`system configuration backup rename`
Visualize os arquivos de backup de configuração de nó e cluster para um ou mais nós no cluster	`system configuration backup show`
Exclua um arquivo de backup de configuração em um nó	`system configuration backup delete` Este comando exclui o arquivo de backup de configuração somente no nó especificado. Se o arquivo de backup de configuração também existir em outros nós no cluster, ele permanecerá nesses nós.

Encontre um arquivo de backup de configuração para usar para recuperar um nó

Você usa um arquivo de backup de configuração localizado em um URL remoto ou em um nó no cluster para recuperar uma configuração de nó.

Sobre esta tarefa

Você pode usar um arquivo de backup de configuração de cluster ou nó para restaurar uma configuração de nó.

Passo

1. Disponibilize o arquivo de backup de configuração para o nó para o qual você precisa restaurar a configuração.

Se o arquivo de backup de configuração estiver localizado…	Então…
Em um URL remoto	Use o `system configuration backup download` comando no nível de privilégio avançado para baixá-lo para o nó de recuperação.
Em um nó no cluster	a. Use o `system configuration backup show` comando no nível de privilégio avançado para exibir a lista de arquivos de backup de configuração disponíveis no cluster que contém a configuração do nó de recuperação. b. Se o arquivo de backup de configuração que você identificar não existir no nó de recuperação, use o `system configuration backup copy` comando para copiá-lo para o nó de recuperação.

Se você recriou o cluster anteriormente, você deve escolher um arquivo de backup de configuração que foi criado após a recriação do cluster. Se você precisar usar um arquivo de backup de configuração que foi criado antes da recriação do cluster, depois de recuperar o nó, você deve recriar o cluster novamente.

Restaure a configuração do nó usando um arquivo de backup de configuração

Você restaura a configuração do nó usando o arquivo de backup de configuração identificado e disponibilizado para o nó de recuperação.

Sobre esta tarefa

Você só deve executar esta tarefa para se recuperar de um desastre que resultou na perda dos arquivos de configuração local do nó.

Passos

1. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Se o nó estiver saudável, no nível de privilégio avançado de um nó diferente, use o `cluster modify`

comando com os `-node` parâmetros e `-eligibility` para marcá-lo inelegível e isolá-lo do cluster.

Se o nó não estiver saudável, então você deve pular esta etapa.

Este exemplo modifica o node2 para ser inelegível para participar do cluster para que sua configuração possa ser restaurada:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Use o `system configuration recovery node restore` comando no nível de privilégio avançado para restaurar a configuração do nó a partir de um arquivo de backup de configuração.

   Se o nó perdeu sua identidade, incluindo seu nome, então você deve usar o `-nodename-in-backup` parâmetro para especificar o nome do nó no arquivo de backup de configuração.

   Este exemplo restaura a configuração do nó usando um dos arquivos de backup de configuração armazenados no nó:

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z

Warning: This command overwrites local configuration files with
         files contained in the specified backup file. Use this
         command only to recover from a disaster that resulted
         in the loss of the local configuration files.
         The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

   A configuração é restaurada e o nó é reiniciado.

4. Se você marcou o nó inelegível, use o `system configuration recovery cluster sync` comando para marcar o nó como qualificado e sincronizá-lo com o cluster.
5. Se você estiver operando em um ambiente SAN, use o `system node reboot` comando para reinicializar o nó e restabelecer o quorum SAN.

Depois de terminar

Se você recriou anteriormente o cluster e se estiver restaurando a configuração do nó usando um arquivo de backup de configuração que foi criado antes da recriação do cluster, você deverá recriar o cluster novamente.

Encontre uma configuração a ser usada para recuperar um cluster

Você usa a configuração de um nó no cluster ou de um arquivo de backup de configuração de cluster para recuperar um cluster.

Passos

1. Escolha um tipo de configuração para recuperar o cluster.

   - Um nó no cluster

Se o cluster consistir em mais de um nó e um dos nós tiver uma configuração de cluster a partir de quando o cluster estava na configuração desejada, então você pode recuperar o cluster usando a configuração armazenada nesse nó.

Na maioria dos casos, o nó que contém o anel de replicação com o ID de transação mais recente é o melhor nó a ser usado para restaurar a configuração do cluster. O `cluster ring show` comando no nível de privilégio avançado permite exibir uma lista dos anéis replicados disponíveis em cada nó no cluster.

- Um arquivo de backup de configuração de cluster

  Se você não conseguir identificar um nó com a configuração correta do cluster ou se o cluster consistir em um único nó, você poderá usar um arquivo de backup de configuração de cluster para recuperar o cluster.

Se você estiver recuperando o cluster de um arquivo de backup de configuração, todas as alterações de configuração feitas desde que o backup foi feito serão perdidas. Você deve resolver quaisquer discrepâncias entre o arquivo de backup de configuração e a configuração atual após a recuperação. Consulte o artigo da base de dados de Conhecimento "Guia de resolução da cópia de segurança da configuração do ONTAP"para obter orientações sobre resolução de problemas.

2. Se você optar por usar um arquivo de backup de configuração de cluster, disponibilize o arquivo para o nó que você planeja usar para recuperar o cluster.

Se o arquivo de backup de configuração estiver localizado…	**Então…**
Em um URL remoto	Use o `system configuration backup download` comando no nível de privilégio avançado para baixá-lo para o nó de recuperação.
Em um nó no cluster	a. Use o `system configuration backup show` comando no nível de privilégio avançado para encontrar um arquivo de backup de configuração de cluster que foi criado quando o cluster estava na configuração desejada. b. Se o arquivo de backup de configuração de cluster não estiver localizado no nó que você pretende usar para recuperar o cluster, use o `system configuration backup copy` comando para copiá-lo para o nó de recuperação.

Restaurar uma configuração de cluster a partir de uma configuração existente

Para restaurar uma configuração de cluster a partir de uma configuração existente após uma falha de cluster, crie novamente o cluster usando a configuração de cluster que você escolheu e disponibilizou para o nó de recuperação e, em seguida, rejunte cada nó adicional ao novo cluster.

Sobre esta tarefa

Você só deve executar essa tarefa para se recuperar de um desastre que resultou na perda da configuração do cluster.

> Se você estiver recriando o cluster a partir de um arquivo de backup de configuração, entre em Contato com o suporte técnico para resolver quaisquer discrepâncias entre o arquivo de backup de configuração e a configuração presente no cluster.
>
> Se você estiver recuperando o cluster de um arquivo de backup de configuração, todas as alterações de configuração feitas desde que o backup foi feito serão perdidas. Você deve resolver quaisquer discrepâncias entre o arquivo de backup de configuração e a configuração atual após a recuperação. Consulte o artigo da base de dados de Conhecimento "Guia de resolução de backup de configuração do ONTAP para orientação de solução de problemas" .

Passos

1. Desativar o failover de storage para cada par de HA:

   `storage failover modify -node` *`node_name`* `-enabled false`

   Você só precisa desativar o failover de storage uma vez para cada par de HA. Quando você desativa o failover de armazenamento para um nó, o failover de armazenamento também é desativado no parceiro do nó.

2. Interrompa cada nó, exceto o nó em recuperação:

   `system node halt -node` *`node_name`* `-reason "text"`

   ```
   cluster1::*> system node halt -node node0 -reason "recovering cluster"

   Warning: Are you sure you want to halt the node? {y|n}: y
   ```

3. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

4. No nó de recuperação, use o **`system configuration recovery cluster recreate`** comando para recriar o cluster.

   Este exemplo recria o cluster usando as informações de configuração armazenadas no nó de recuperação:

   ```
   cluster1::*> configuration recovery cluster recreate -from node

   Warning: This command will destroy your existing cluster. It will
            rebuild a new single-node cluster consisting of this node
            and its current configuration. This feature should only be
            used to recover from a disaster. Do not perform any other
            recovery operations while this operation is in progress.
   Do you want to continue? {y|n}: y
   ```

Um novo cluster é criado no nó de recuperação.

5. Se você estiver recriando o cluster a partir de um arquivo de backup de configuração, verifique se a recuperação do cluster ainda está em andamento:

   system configuration recovery cluster show

   Não é necessário verificar o estado de recuperação do cluster se estiver recriando o cluster a partir de um nó íntegro.

   ```
   cluster1::*> system configuration recovery cluster show
    Recovery Status: in-progress
    Is Recovery Status Persisted: false
   ```

6. Inicialize cada nó que precisa ser reUnido ao cluster recriado.

   É necessário reinicializar os nós um de cada vez.

7. Para cada nó que precisa ser Unido ao cluster recriado, faça o seguinte:

   a. A partir de um nó íntegro no cluster recriado, junte-se novamente ao nó de destino:

      system configuration recovery cluster rejoin -node *node_name*

      Este exemplo rejura o nó de destino "'node2"" para o cluster recriado:

      ```
      cluster1::*> system configuration recovery cluster rejoin -node node2

      Warning: This command will rejoin node "node2" into the local
               cluster, potentially overwriting critical cluster
               configuration files. This command should only be used
               to recover from a disaster. Do not perform any other
               recovery operations while this operation is in progress.
               This command will cause node "node2" to reboot.
      Do you want to continue? {y|n}: y
      ```

      O nó de destino é reinicializado e, em seguida, se junta ao cluster.

   b. Verifique se o nó de destino está íntegro e formou quórum com o restante dos nós no cluster:

      cluster show -eligibility true

      O nó de destino deve voltar a juntar-se ao cluster recriado antes de poder voltar a aderir a outro nó.

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. Se você criou novamente o cluster a partir de um arquivo de backup de configuração, defina o status de recuperação para ser concluído:

   `system configuration recovery cluster modify -recovery-status complete`

9. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

10. Se o cluster consistir em apenas dois nós, use o **`cluster ha modify`** comando para reativar a HA do cluster.
11. Use o **`storage failover modify`** comando para reativar o failover de storage para cada par de HA.

Depois de terminar

Se o cluster tiver relacionamentos de pares SnapMirror, você também precisará recriar esses relacionamentos. Para obter mais informações, "Proteção de dados"consulte .

Sincronize um nó com o cluster

Se houver quorum em todo o cluster, mas um ou mais nós estiverem fora de sincronia com o cluster, será necessário sincronizar o nó para restaurar o banco de dados replicado (RDB) no nó e colocá-lo no quorum.

Passo

1. A partir de um nó saudável, use o `system configuration recovery cluster sync` comando no nível de privilégio avançado para sincronizar o nó que está fora de sincronia com a configuração do cluster.

   Este exemplo sincroniza um nó (*node2*) com o resto do cluster:

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

Resultado

O RDB é replicado para o nó e o nó se torna elegível para participar do cluster.

Gerenciar despejos principais (somente administradores de cluster) no ONTAP

Quando um nó entra em pânico, um despejo de núcleo ocorre e o sistema cria um arquivo de despejo de núcleo que o suporte técnico pode usar para solucionar o problema. Você pode configurar ou exibir atributos de despejo de memória. Você também pode salvar, exibir, segmentar, carregar ou excluir um arquivo de despejo de memória.

Você pode gerenciar despejos principais das seguintes maneiras:

- Configurar os despejos principais e exibir as configurações
- Exibindo informações básicas, o status e os atributos dos despejos principais

  Os arquivos e relatórios de despejo de memória são armazenados `/mroot/etc/crash/` no diretório de um nó. Você pode exibir o conteúdo do diretório usando os `system node coredump` comandos ou um navegador da Web.

- Salvando o conteúdo do despejo do núcleo e carregando o arquivo salvo em um local especificado ou no suporte técnico

  O ONTAP impede que você inicie o salvamento de um arquivo de despejo de memória durante uma aquisição, uma realocação agregada ou um giveback.

- Excluindo arquivos de despejo de memória que não são mais necessários

Comandos para gerenciar despejos principais

Você usa os `system node coredump config` comandos para gerenciar a configuração de despejos de núcleo, os `system node coredump` comandos para gerenciar os arquivos de despejo de núcleo e os `system node coredump reports` comandos para gerenciar relatórios de núcleo de aplicativos.

Saiba mais sobre os comandos descritos neste tópico no "Referência do comando ONTAP".

Se você quiser…	Use este comando…
Configurar despejos de núcleo	`system node coredump config modify`
Apresentar as definições de configuração para despejos de núcleo	`system node coredump config show`
Exibir informações básicas sobre despejos de núcleo	`system node coredump show`
Acione manualmente um despejo de memória quando você reiniciar um nó	`system node reboot` com ambos `-dump` os parâmetros e `-skip-lif-migration-before -reboot` O parâmetro link:https://docs.NetApp.com/US-en/ONTAP-cli//system-node-reboot.html[`skip-lif-migration-before-reboot` especifica que a migração de LIF antes de uma reinicialização será ignorada.
Acione manualmente um despejo de núcleo quando você desligar um nó	`system node halt` com ambos `-dump` os parâmetros e `-skip-lif-migration-before -shutdown` O parâmetro link:https://docs.NetApp.com/US-en/ONTAP-cli/system-node-halt.html[`skip-lif-migration-before-shutdown` especifica que a migração de LIF antes de um desligamento será ignorada.
Salve um despejo de memória especificado	`system node coredump save`
Salve todos os despejos de núcleo não salvos que estão em um nó especificado	`system node coredump save-all`
Gere e envie uma mensagem AutoSupport com um arquivo de despejo de memória que você especificar	`system node autosupport invoke-core-upload` O `-uri` parâmetro opcional especifica um destino alternativo para a mensagem AutoSupport.

Se você quiser…	Use este comando…
Exibir informações de status sobre os despejos do núcleo	`system node coredump status`
Exclua um despejo de memória especificado	`system node coredump delete`
Exclua todos os despejos de núcleo não salvos ou todos os arquivos de núcleo salvos em um nó	`system node coredump delete-all`
Exibir relatórios de despejo do núcleo do aplicativo	`system node coredump reports show`
Excluir um relatório de despejo do núcleo do aplicativo	`system node coredump reports delete`

Informações relacionadas

"Referência do comando ONTAP"

Gerenciamento de disco e camada (agregado)

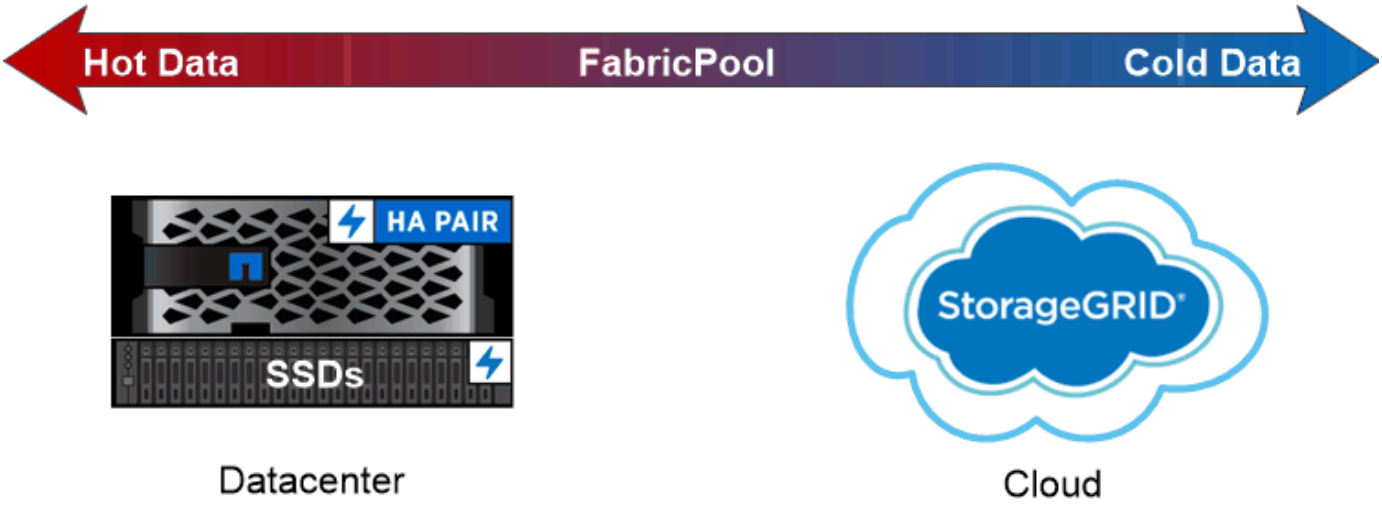
Visão geral de discos e camadas locais (agregados)

Você pode gerenciar o storage físico do ONTAP usando o Gerenciador do sistema e a CLI. Você pode criar, expandir e gerenciar camadas locais (agregados), trabalhar com camadas locais (agregados) do Flash Pool, gerenciar discos e gerenciar políticas de RAID.

Quais são os níveis locais (agregados)

Níveis locais (também chamados de *agregados*) são contentores para os discos gerenciados por um nó. Use as camadas locais para isolar workloads com demandas de desempenho diferentes, categorizar dados com padrões de acesso diferentes ou separar dados para fins regulatórios.

- Para aplicações essenciais aos negócios que precisam da menor latência possível e da maior performance possível, você pode criar um nível local que consiste inteiramente de SSDs.
- Para categorizar dados com diferentes padrões de acesso, você pode criar um *nível local híbrido*, implantando flash como cache de alto desempenho para um conjunto de dados em funcionamento, ao mesmo tempo em que usa HDDs de baixo custo ou storage de objetos para dados acessados com menos frequência.
  - Um *Flash Pool* consiste em SSDs e HDDs.
  - Um *FabricPool* consiste em um nível local totalmente SSD com um armazenamento de objetos anexado.
- Se você precisar separar os dados arquivados de dados ativos para fins regulatórios, poderá usar um nível local que consiste em HDDs de capacidade ou uma combinação de HDDs de desempenho e capacidade.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

Trabalhando com camadas locais (agregados)

Você pode executar as seguintes tarefas:

- "Gerenciar camadas locais (agregados)"
- "Gerenciar discos"
- "Gerenciar configurações RAID"
- "Gerenciar camadas do Flash Pool"

Você executa essas tarefas se as seguintes tarefas forem verdadeiras:

- Você não quer usar uma ferramenta de script automatizado.
- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você tem uma configuração do MetroCluster e segue os procedimentos descritos "MetroCluster"na documentação para configuração inicial e diretrizes para camadas locais (agregados) e gerenciamento de disco.

Informações relacionadas

- "Gerenciar categorias de nuvem do FabricPool"

Gerenciar camadas locais (agregados)

Gerenciar camadas locais (agregados)

Use o Gerenciador do sistema ou a CLI do ONTAP para adicionar camadas locais (agregados), gerenciar seu uso e adicionar capacidade (discos) a elas.

Você pode executar as seguintes tarefas:

- "Adicionar (criar) um nível local (agregado)"

  Para adicionar um nível local, você segue um fluxo de trabalho específico. Você determina o número de discos ou partições de disco que você precisa para o nível local e decide qual método usar para criar o nível local. Você pode adicionar níveis locais automaticamente permitindo que o ONTAP atribua a configuração ou especifique manualmente a configuração.

- "Gerenciar o uso de camadas locais (agregados)"

  Para os níveis locais existentes, você pode renomeá-los, definir seus custos de Mídia ou determinar suas informações de unidade e grupo RAID. É possível modificar a configuração RAID de uma camada local e atribuir camadas locais a VMs de storage (SVMs). É possível modificar a configuração RAID de uma camada local e atribuir camadas locais a VMs de storage (SVMs). É possível determinar quais volumes residem em um nível local e quanto espaço eles usam em um nível local. Você pode controlar quanto espaço os volumes podem usar. Você pode realocar a propriedade do nível local com um par de HA. Você também pode excluir um nível local.

- "Adicionar capacidade (discos) a um nível local (agregado)"

  Usando métodos diferentes, você segue um fluxo de trabalho específico para adicionar capacidade. É possível adicionar discos a uma camada local e adicionar unidades a um nó ou compartimento. Se necessário, você pode corrigir partições sobressalentes desalinhadas.

Adicionar (criar) um nível local (agregado)

Adicionar um nível local (criar um agregado)

Para adicionar um nível local (criar um agregado), você segue um fluxo de trabalho específico.

Você determina o número de discos ou partições de disco que você precisa para o nível local e decide qual método usar para criar o nível local. Você pode adicionar níveis locais automaticamente permitindo que o ONTAP atribua a configuração ou especifique manualmente a configuração.

- "Fluxo de trabalho para adicionar um nível local (agregado)"
- "Determinar o número de discos ou partições de disco necessárias para um nível local (agregado)"
- "Decida qual método de criação de nível local (agregado) usar"
- "Adicionar camadas locais (agregados) automaticamente"
- "Adicione camadas locais (agregados) manualmente"

Fluxo de trabalho para adicionar um nível local (agregado)

A criação de camadas locais (agregados) fornece storage para volumes no sistema.

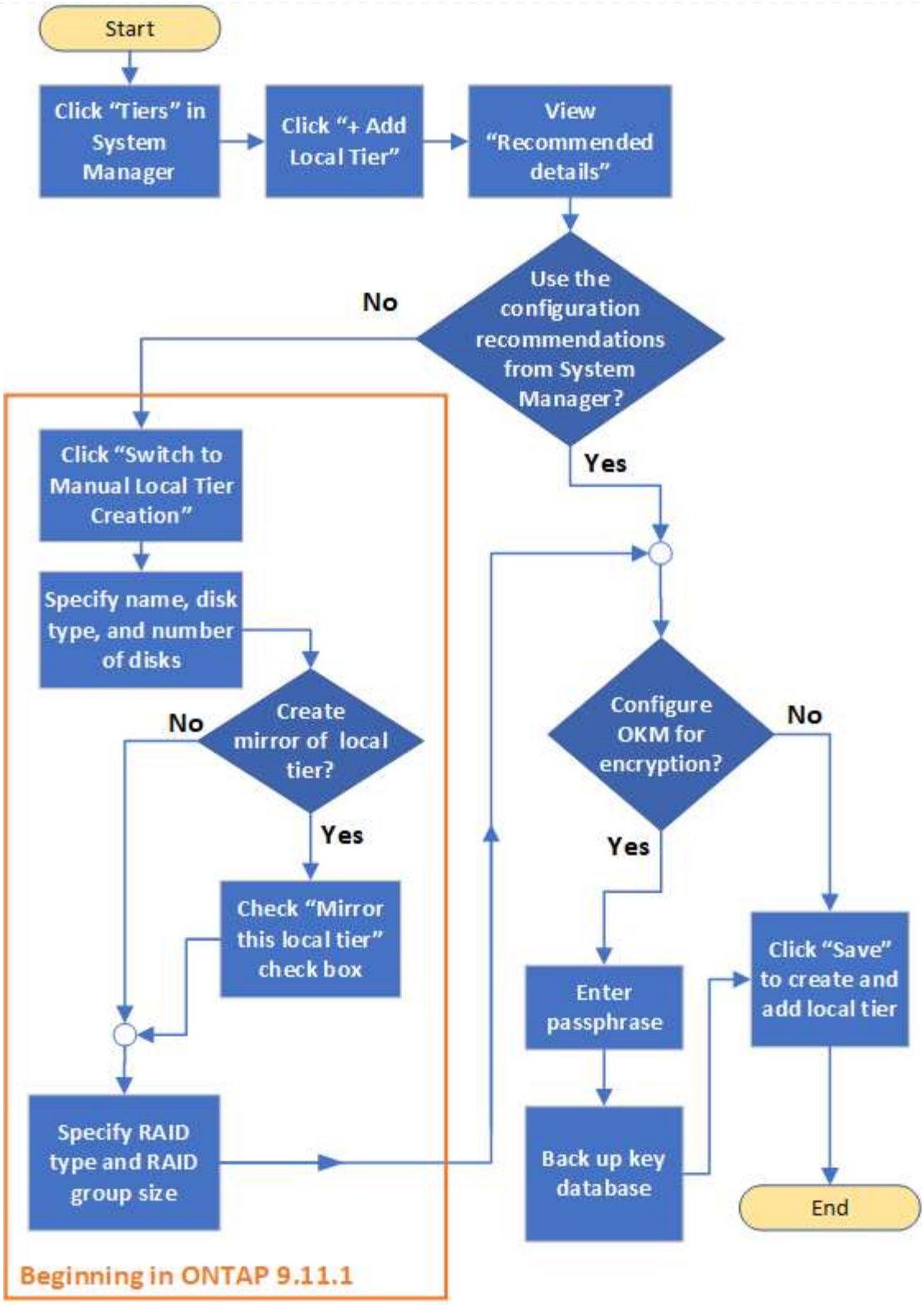
O fluxo de trabalho para criar camadas locais (agregados) é específico para a interface que você usa - System Manager ou CLI:

Fluxo de trabalho do System Manager

Use o System Manager para adicionar (criar) um nível local

O System Manager cria camadas locais com base nas práticas recomendadas para a configuração de camadas locais.

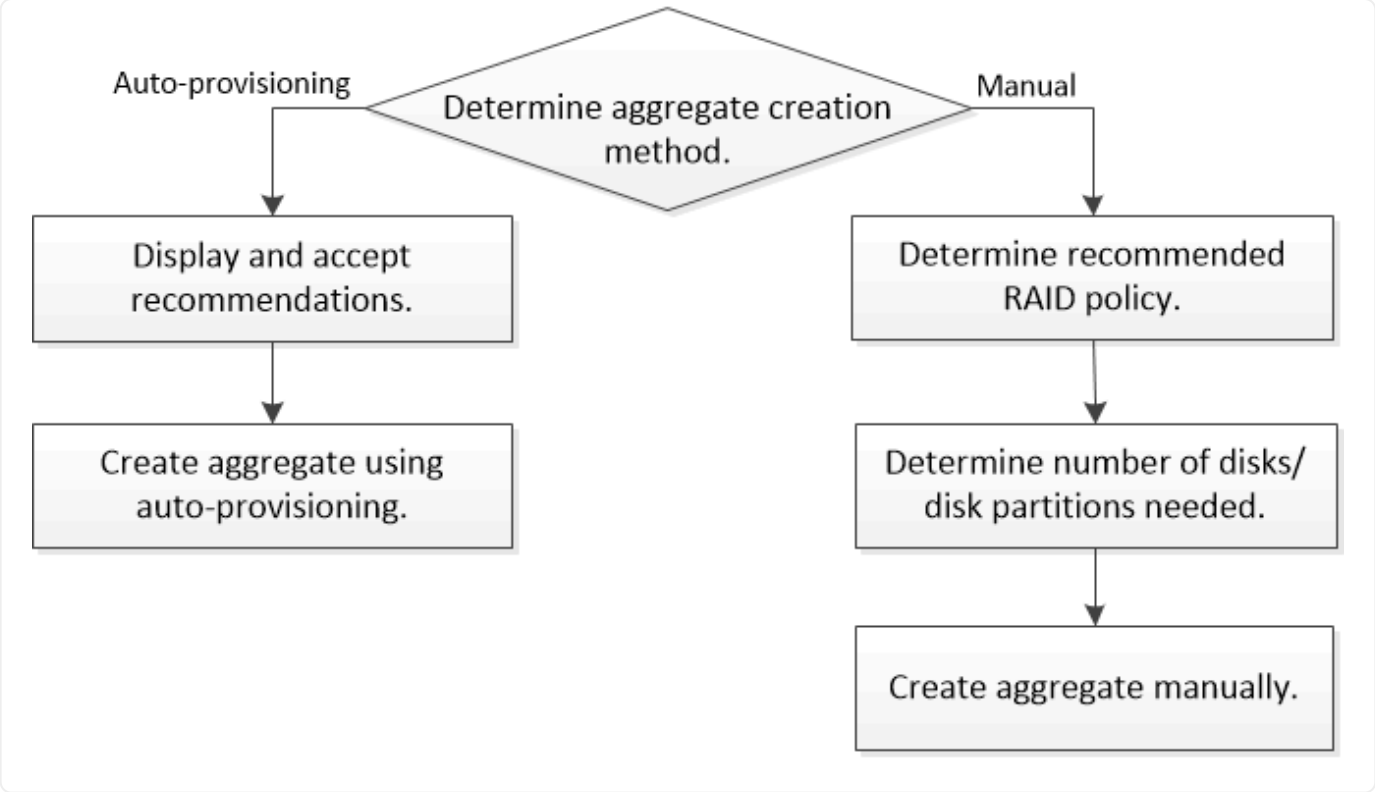
A partir do ONTAP 9.11,1, você pode decidir configurar níveis locais manualmente se quiser uma configuração diferente da recomendada durante o processo automático para adicionar um nível local.



Fluxo de trabalho da CLI

Use a CLI para adicionar (criar) um agregado

A partir do ONTAP 9.2, o ONTAP pode fornecer configurações recomendadas ao criar agregados (provisionamento automático). Se as configurações recomendadas, baseadas nas práticas recomendadas, forem apropriadas no seu ambiente, você poderá aceitá-las para criar os agregados. Caso contrário, você pode criar agregados manualmente.



Determinar o número de discos ou partições de disco necessárias para um nível local (agregado)

Você precisa ter discos ou partições de disco suficientes no seu nível local (agregado) para atender aos requisitos de sistema e negócios. Você também deve ter o número recomendado de discos hot spare ou partições de disco hot spare para minimizar o potencial de perda de dados.

O particionamento de dados raiz é ativado por padrão em determinadas configurações. Sistemas com particionamento de dados raiz habilitado usam partições de disco para criar camadas locais. Os sistemas que não têm o particionamento de dados raiz ativado utilizam discos não particionados.

Você precisa ter discos ou partições de disco suficientes para atender ao número mínimo necessário para sua política de RAID e o suficiente para atender aos requisitos mínimos de capacidade.

No ONTAP, o espaço utilizável da unidade é menor que a capacidade física da unidade. É possível encontrar o espaço utilizável de uma unidade específica e o número mínimo de discos ou partições de disco necessários para cada política RAID no "Hardware Universe".

Determine o espaço utilizável de um disco específico

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para determinar o espaço utilizável dos discos

Execute as seguintes etapas para exibir o tamanho utilizável de um disco:

Passos

1. Vá para **Storage > Tiers**
2. Clique ⋮ ao lado do nome do nível local.
3. Selecione a guia **informações do disco**.

CLI

Use a CLI para determinar o espaço utilizável dos discos

Execute a seguinte etapa para exibir o tamanho utilizável de um disco:

Passo

1. Apresentar informações sobre o disco sobressalente:

```
storage aggregate show-spare-disks
```

Além do número de discos ou partições de disco necessárias para criar seu grupo RAID e atender aos requisitos de capacidade, você também deve ter o número mínimo de discos hot spare ou partições de disco hot spare recomendadas para seu agregado:

- Para agregados all-flash, você deve ter no mínimo um disco hot spare ou partição de disco.

  ⓘ O padrão do AFF C190 é sem unidade sobressalente. Esta exceção é totalmente suportada.

- Para agregados homogêneos não flash, você deve ter no mínimo dois discos hot spare ou partições de disco.
- Para pools de storage SSD, você deve ter no mínimo um disco hot spare para cada par de HA.
- Para agregados Flash Pool, você deve ter no mínimo dois discos sobressalente para cada par de HA. Você pode encontrar mais informações sobre as políticas RAID compatíveis para agregados Flash Pool no "Hardware Universe".
- Para dar suporte ao uso do Centro de Manutenção e evitar problemas causados por várias falhas de disco simultâneas, você deve ter no mínimo quatro hot spares em operadoras de vários discos.

Informações relacionadas

"NetApp Hardware Universe"

"Relatório técnico da NetApp 3838: Guia de configuração do subsistema de armazenamento"

Decidir qual método usar para criar camadas locais (agregados)

Embora o ONTAP forneça recomendações de práticas recomendadas para adicionar camadas locais automaticamente (criando agregados com provisionamento automático), é necessário determinar se as configurações recomendadas são compatíveis com o seu

ambiente. Se não estiverem, você deverá tomar decisões sobre a política de RAID e a configuração de disco e, em seguida, criar manualmente as camadas locais.

Quando um nível local é criado automaticamente, o ONTAP analisa os discos sobressalentes disponíveis no cluster e gera uma recomendação sobre como os discos sobressalentes devem ser usados para adicionar camadas locais de acordo com as práticas recomendadas. O ONTAP exibe as configurações recomendadas. Você pode aceitar as recomendações ou adicionar manualmente os níveis locais.

Antes de aceitar as recomendações do ONTAP

Se alguma das seguintes condições de disco estiver presente, elas devem ser abordadas antes de aceitar as recomendações do ONTAP:

- Discos em falta
- Flutuação nos números de disco sobressalente
- Discos não atribuídos
- Peças sobressalentes não zeradas
- Discos submetidos a testes de manutenção

A `storage aggregate auto-provision` página de manual contém mais informações sobre esses requisitos.

Quando tem de utilizar o método manual

Em muitos casos, o layout recomendado do nível local será ideal para o seu ambiente. No entanto, se o cluster estiver executando o ONTAP 9.1 ou anterior, ou se o ambiente incluir as configurações a seguir, será necessário criar o nível local usando o método manual.

> A partir do ONTAP 9.11,1, você pode adicionar manualmente camadas locais com o Gerenciador de sistema.

- Agregados usando LUNs de array de terceiros
- Discos virtuais com Cloud Volumes ONTAP ou ONTAP Select
- Sistema MetroCluster
- SyncMirror
- Discos MSATA
- Camadas do FlashPool (agregados)
- Vários tipos ou tamanhos de disco são conetados ao nó

Selecione o método para criar camadas locais (agregados)

Escolha o método que deseja usar:

- "Adicionar (criar) camadas locais (agregados) automaticamente"
- "Adicione (crie) camadas locais (agregados) manualmente"

Informações relacionadas

- "Referência do comando ONTAP"

Adicionar camadas locais automaticamente (criar agregados com provisionamento automático) no ONTAP

Se a recomendação de práticas recomendadas fornecida pelo ONTAP para adicionar automaticamente um nível local (criar um agregado com provisionamento automático) for apropriada no seu ambiente, você poderá aceitar a recomendação e permitir que o ONTAP adicione o nível local.

Antes de começar

Os discos devem ser de propriedade de um nó antes que possam ser usados em um nível local (agregado). Se o cluster não estiver configurado para usar atribuição automática de propriedade de disco, você deverá "atribuir propriedade manualmente".

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

System Manager

Passos

1. No System Manager, clique em **Storage > Tiers**.
2. Na página **níveis**, clique + Add Local Tier para criar um novo nível local:

   A página **Adicionar nível local** mostra o número recomendado de níveis locais que podem ser criados nos nós e o armazenamento utilizável disponível.

3. Clique em **Detalhes recomendados** para visualizar a configuração recomendada pelo System Manager.

   O Gerenciador do sistema exibe as seguintes informações começando com ONTAP 9.8:

   - **Nome do nível local** (você pode editar o nome do nível local começando com ONTAP 9.10,1)
   - **Nome do nó**
   - * Tamanho utilizável *
   - **Tipo de armazenamento**

     A partir de ONTAP 9.10,1, são apresentadas informações adicionais:

   - **Disks**: Mostrando o número, o tamanho e o tipo dos discos
   - **Layout**: Mostrando o layout do grupo RAID, incluindo quais discos são paridade ou dados e quais slots não são utilizados.
   - **Discos sobressalentes**: Mostrando o nome do nó, o número e o tamanho dos discos sobressalentes e o tipo de armazenamento.

4. Execute um dos seguintes passos:

Se você quiser…	Então faça isso…
Aceite as recomendações do System Manager.	Prossiga para A etapa para configurar o Gerenciador de chaves integrado para criptografia.
Configure manualmente os níveis locais e ***not*** Use as recomendações do System Manager.	Avance para "Adicione um nível local (criar agregado) manualmente": • Para o ONTAP 9.10,1 e versões anteriores, siga as etapas para usar a CLI. • A partir do ONTAP 9.11,1, siga os passos para utilizar o Gestor do sistema.

5. (Opcional): Se o Gerenciador de chaves integrado tiver sido instalado, você pode configurá-lo para criptografia. Marque a caixa de seleção **Configure Onboard Key Manager for Encryption** (Configurar o Gerenciador de chaves integrado para criptografia).
   a. Introduza uma frase-passe.
   b. Introduza novamente a frase-passe para a confirmar.
   c. Salve a senha para uso futuro caso o sistema precise ser recuperado.

d. Faça backup do banco de dados de chaves para uso futuro.

6. Clique em **Salvar** para criar o nível local e adicioná-lo à sua solução de storage.

CLI

Você executa o `storage aggregate auto-provision` comando para gerar recomendações de layout agregado. Em seguida, você pode criar agregados depois de analisar e aprovar recomendações do ONTAP.

O que você vai precisar

O ONTAP 9.2 ou posterior deve estar em execução no cluster.

Sobre esta tarefa

O resumo padrão gerado com o `storage aggregate auto-provision` comando lista os agregados recomendados a serem criados, incluindo nomes e tamanho utilizável. Você pode exibir a lista e determinar se deseja criar os agregados recomendados quando solicitado.

Você também pode exibir um resumo detalhado usando a `-verbose` opção, que exibe os seguintes relatórios:

- Resumo por nó de novos agregados para criar, descobrir peças sobressalentes e discos e partições sobressalentes restantes após a criação de agregados
- Novos agregados de dados para criar com contagens de discos e partições a serem usadas
- Layout do grupo RAID mostrando como discos e partições sobressalentes serão usados em novos agregados de dados a serem criados
- Detalhes sobre discos sobressalentes e partições restantes após a criação de agregados

Se você estiver familiarizado com o método de provisão automática e seu ambiente estiver corretamente preparado, você pode usar a `-skip-confirmation` opção para criar o agregado recomendado sem exibição e confirmação. O `storage aggregate auto-provision` comando não é afetado pela configuração da sessão CLI `-confirmations`.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/storage-aggregate-auto-provision.html[`storage aggregate auto-provision` em referência de comando ONTAP.

Passos

1. Execute o `storage aggregate auto-provision` comando com as opções de exibição desejadas.
   - sem opções: Apresentar resumo padrão
   - `-verbose` Opção: Exibir resumo detalhado
   - `-skip-confirmation` Opção: Crie agregados recomendados sem exibição ou confirmação
2. Execute um dos seguintes passos:

Se você quiser…	Então faça isso…

Aceite as recomendações da ONTAP.	Revise a exibição dos agregados recomendados e responda ao prompt para criar os agregados recomendados.
	
	`myA400-44556677::> storage aggregate auto-provision`
	`Node New Data Aggregate Usable Size`
	`---`
	`--- ---`
	`myA400-364 myA400_364_SSD_1 3.29TB`
	`myA400-363 myA400_363_SSD_1 1.46TB`
	`---`
	`--- ---`
	`Total: 2 new data aggregates 4.75TB`
	
	`Do you want to create recommended aggregates? {y`

n}: y Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress. myA400-44556677::> ----	Configure manualmente os níveis locais e ***not*** Use as recomendações do ONTAP.

Informações relacionadas

- "Referência do comando ONTAP"

Adicionar camadas locais (criar agregados) manualmente

Se você não quiser adicionar um nível local (criar um agregado) usando as recomendações de práticas recomendadas do ONTAP, execute o processo manualmente.

Antes de começar

Os discos devem ser de propriedade de um nó antes que possam ser usados em um nível local (agregado). Se o cluster não estiver configurado para usar atribuição automática de propriedade de disco, você deverá "atribuir propriedade manualmente".

System Manager

A partir do ONTAP 9.11,1, se você não quiser usar a configuração recomendada pelo Gerenciador de sistema para criar um nível local, você pode especificar a configuração desejada.

Passos

1. No System Manager, clique em **Storage > Tiers**.
2. Na página **níveis**, clique + Add Local Tier para criar um novo nível local:

   A página **Adicionar nível local** mostra o número recomendado de níveis locais que podem ser criados nos nós e o armazenamento utilizável disponível.

3. Quando o System Manager exibir a recomendação de armazenamento para o nível local, clique em **mudar para criação Manual de nível local** na seção **discos sobressalentes**.

   A página **Adicionar nível local** exibe os campos que você usa para configurar o nível local.

4. Na primeira seção da página **Adicionar nível local**, complete o seguinte:
   a. Introduza o nome do nível local.
   b. (Opcional): Marque a caixa de seleção **Espelhar este nível local** se quiser espelhar o nível local.
   c. Selecione um tipo de disco.
   d. Selecione o número de discos.
5. Na seção **Configuração RAID**, complete o seguinte:
   a. Selecione o tipo RAID.
   b. Selecione o tamanho do grupo RAID.
   c. Clique em Alocação RAID para ver como os discos são alocados no grupo.
6. (Opcional): Se o Gerenciador de chaves integrado tiver sido instalado, você pode configurá-lo para criptografia na seção **criptografia** da página. Marque a caixa de seleção **Configure Onboard Key Manager for Encryption** (Configurar o Gerenciador de chaves integrado para criptografia).
   a. Introduza uma frase-passe.
   b. Introduza novamente a frase-passe para a confirmar.
   c. Salve a senha para uso futuro caso o sistema precise ser recuperado.
   d. Faça backup do banco de dados de chaves para uso futuro.
7. Clique em **Salvar** para criar o nível local e adicioná-lo à sua solução de storage.

CLI

Antes de criar agregados manualmente, você deve revisar as opções de configuração de disco e simular a criação.

Em seguida, você pode emitir o `storage aggregate create` comando e verificar os resultados.

O que você vai precisar

Você deve ter determinado o número de discos e o número de discos hot spare necessários no agregado.

Sobre esta tarefa

Se o particionamento de dados-raiz estiver ativado e você tiver 24 unidades de estado sólido (SSDs) ou

menos em sua configuração, é recomendável que suas partições de dados sejam atribuídas a diferentes nós.

O procedimento para criar agregados em sistemas com particionamento de dados raiz e particionamento de dados raiz ativado é o mesmo que o procedimento para criar agregados em sistemas que utilizam discos não particionados. Se o particionamento de dados raiz estiver ativado no seu sistema, você deve usar o número de partições de disco para a `-diskcount` opção. Para o particionamento root-data-data, a `-diskcount` opção especifica a contagem de discos a serem usados.

> Ao criar vários agregados para uso com FlexGroups, os agregados devem ter o tamanho mais próximo possível.

A `storage aggregate create` página de manual contém mais informações sobre opções e requisitos de criação agregada.

Passos

1. Veja a lista de partições de disco sobressalente para verificar se você tem o suficiente para criar seu agregado:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   As partições de dados são exibidas em `Local Data Usable`. Uma partição raiz não pode ser usada como sobressalente.

2. Simule a criação do agregado:

   ```
   storage aggregate create -aggregate aggregate_name -node node_name
   -raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
   ```

3. Se algum aviso for exibido no comando simulado, ajuste o comando e repita a simulação.
4. Criar o agregado:

   ```
   storage aggregate create -aggregate aggr_name -node node_name -raidtype
   raid_dp -diskcount number_of_disks_or_partitions
   ```

5. Exiba o agregado para verificar se ele foi criado:

   ```
   storage aggregate show-status aggregate_name
   ```

Informações relacionadas

- "Referência do comando ONTAP"

Gerenciar o uso de camadas locais (agregados)

Gerenciar o uso de camadas locais (agregados)

Depois de criar camadas locais (agregados), é possível gerenciar como elas são usadas.

Você pode executar as seguintes tarefas:

- "Renomear um nível local (agregado)"

- "Definir o custo de Mídia de um nível local (agregado)"
- "Determinar informações de unidade e grupo RAID para um nível local (agregado)"
- "Atribuir camadas locais (agregados) a VMs de storage (SVMs)"
- "Determinar quais volumes residem em um nível local (agregado)"
- "Determinar e controlar os usos de espaço de um volume em um nível local (agregado)"
- "Determinar o uso de espaço em um nível local (agregado)"
- "Realocar a propriedade do nível local (agregado) dentro de um par de HA"
- "Excluir um nível local (agregado)"

Renomear um nível local (agregado)

Você pode renomear um nível local (agregado). O método que você segue depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para renomear um nível local (agregado)

A partir de ONTAP 9.10,1, você pode modificar o nome de um nível local (agregado).

Passos

1. No System Manager, clique em **Storage > Tiers**.
2. Clique ⋮ ao lado do nome do nível local.
3. Selecione **Renomear**.
4. Especifique um novo nome para o nível local.

CLI

Use a CLI para renomear um nível local (agregado)

Passo

1. Usando a CLI, renomeie o nível local (agregado):

   `storage aggregate rename -aggregate` *`aggr-name`* `-newname` *`aggr-new-name`*

   O exemplo a seguir renomeia um agregado chamado "aggr5" como "Ales-aggr":

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

Definir o custo de Mídia de um nível local (agregado)

A partir do ONTAP 9.11,1, você pode usar o Gerenciador do sistema para definir o custo de Mídia de um nível local (agregado).

Passos

1. No System Manager, clique em **Storage > Tiers** e, em seguida, clique em **Set Media Cost** (Definir custo

de Mídia*) nos blocos de nível local desejado (agregado).

2. Selecione **camadas ativas e inativas** para ativar a comparação.
3. Introduza um tipo de moeda e um montante.

Quando introduz ou altera o custo do material, a alteração é efetuada em todos os tipos de material.

Manualmente Fast zero drives

Em sistemas recém-instalados com o ONTAP 9.4 ou posterior e sistemas reinicializados com o ONTAP 9.4 ou posterior, *fast zero* é usado para zero unidades.

Com *fast zero*, as unidades são zeradas em segundos. Isso é feito automaticamente antes do provisionamento e reduz bastante o tempo necessário para inicializar o sistema, criar agregados ou expandir agregados quando unidades sobressalentes são adicionadas.

A restauração rápida é suportada em SSDs e HDDs.

> *A restauração rápida* não é suportada em sistemas atualizados a partir do ONTAP 9.3 ou anterior. O ONTAP 9.4 ou posterior deve ser instalado recentemente ou o sistema deve ser reinicializado. No ONTAP 9.3 e versões anteriores, as unidades também são zeradas automaticamente pelo ONTAP. No entanto, o processo leva mais tempo.

Se você precisar zerar manualmente uma unidade, você pode usar um dos seguintes métodos. No ONTAP 9.4 e posterior, a restauração manual de uma unidade também leva apenas segundos.

Comando CLI

Use um comando CLI para acelerar a zero unidades

Sobre esta tarefa

Admin Privileges são necessários para usar este comando.

Passos

1. Digite o comando CLI:

```
storage disk zerospares
```

Opções do menu de inicialização

Selecione as opções no menu de inicialização para unidades de zero rápido

Sobre esta tarefa

- O aprimoramento de restauração rápida não suporta sistemas atualizados de uma versão anterior ao ONTAP 9.4.
- Se qualquer nó no cluster contiver um nível local (agregado) com unidades de zeragem rápida, não será possível reverter o cluster para o ONTAP 9.2 ou anterior.

Passos

1. No menu de inicialização, selecione uma das seguintes opções:
   - (4) limpe a configuração e inicialize todos os discos
   - (9a) Desparticionar todos os discos e remover suas informações de propriedade
   - (9b) limpe a configuração e inicialize o nó com discos inteiros

Atribua manualmente a propriedade do disco

Os discos devem ser de propriedade de um nó antes que possam ser usados em um nível local (agregado).

Sobre esta tarefa

- Se você estiver atribuindo manualmente a propriedade de um par de HA que não está sendo inicializado e não tiver apenas DS460C gavetas, use a opção 1.
- Se você estiver inicializando um par de HA com apenas DS460C gavetas, use a opção 2 para atribuir manualmente a propriedade para as unidades raiz.

Opção 1: Maioria dos pares de HA

Para um par de HA que não está sendo inicializado e não tem apenas DS460C gavetas, use este procedimento para atribuir manualmente a propriedade.

Sobre esta tarefa

- Os discos para os quais você está atribuindo propriedade devem estar em uma gaveta que esteja fisicamente cabeada para o nó ao qual você está atribuindo propriedade.
- Se você estiver usando discos em um nível local (agregado):
  - Os discos devem ser de propriedade de um nó antes que possam ser usados em um nível local (agregado).
  - Não é possível reatribuir a propriedade de um disco que esteja em uso em um nível local (agregado).

Passos

1. Use a CLI para exibir todos os discos não possuídos:

   ```
   storage disk show -container-type unassigned
   ```

2. Atribuir cada disco:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   Você pode usar o caractere curinga para atribuir mais de um disco de uma vez. Se você estiver reatribuindo um disco sobressalente que já é de propriedade de um nó diferente, você deve usar a opção "'-force".

Opção 2: Um par de HA com apenas DS460C gavetas

Para um par de HA que você está inicializando e que tenha apenas DS460C gavetas, use este procedimento para atribuir manualmente a propriedade das unidades raiz.

Sobre esta tarefa

- Ao inicializar um par de HA que tenha apenas DS460C gavetas, você deve atribuir manualmente as unidades raiz para estar em conformidade com a política de meia gaveta.

  Após a inicialização do par de HA (inicialização), a atribuição automática da propriedade do disco é ativada automaticamente e usa a política de meia gaveta para atribuir propriedade às unidades restantes (exceto as unidades raiz) e a quaisquer unidades adicionadas no futuro, como a substituição de discos com falha, a resposta a uma mensagem de "peças sobressalentes baixas" ou a adição de capacidade.

  Saiba mais sobre a política de meia gaveta no "Sobre a atribuição automática de propriedade de disco"tópico .

- O RAID precisa de um mínimo de 10 unidades para cada par de HA (5 TB para cada nó) para quaisquer unidades NL-SAS superiores a 8TB TB em uma gaveta de DS460C TB.

Passos

1. Se as DS460C gavetas não estiverem totalmente preenchidas, execute as seguintes etapas; caso contrário, vá para a próxima etapa.

   a. Primeiro, instale unidades na linha dianteira (compartimentos de unidades 0, 3, 6 e 9) de cada gaveta.

      A instalação de acionamentos na fila dianteira de cada gaveta permite um fluxo de ar adequado e evita o superaquecimento.

   b. Para as unidades restantes, distribua-as uniformemente em cada gaveta.

      Encha as linhas da gaveta da frente para trás. Se você não tiver unidades suficientes para preencher linhas, instale-as em pares para que as unidades ocupem o lado esquerdo e direito de uma gaveta uniformemente.

      A ilustração a seguir mostra a numeração do compartimento de unidades e os locais em uma gaveta DS460C.

2. Faça login no clustershell usando o LIF de gerenciamento de nó ou LIF de gerenciamento de cluster.
3. Atribua manualmente as unidades raiz em cada gaveta para estar em conformidade com a política de meia gaveta usando as seguintes subetapas:

   A política de meia gaveta atribui a metade esquerda das unidades de uma gaveta (compartimentos 0 a 5) ao nó A e a metade direita das unidades de uma gaveta (compartimentos 6 a 11) ao nó B.

   a. Exibir todos os discos não possuídos:
   `storage disk show -container-type unassigned`
   b. Atribuir os discos raiz:
   `storage disk assign -disk disk_name -owner owner_name`

      Você pode usar o caractere curinga para atribuir mais de um disco de cada vez.

Determinar informações de unidade e grupo RAID para um nível local (agregado)

Algumas tarefas de administração de camadas locais (agregadas) exigem que você saiba quais tipos de unidades compõem o nível local, seu tamanho, checksum e status, se eles são compartilhados com outros níveis locais e o tamanho e a composição dos grupos RAID.

Passo

1. Mostrar as unidades para o agregado, por grupo RAID:

   `storage aggregate show-status` *`aggr_name`*

   As unidades são exibidas para cada grupo RAID no agregado.

   Você pode ver o tipo RAID da unidade (dados, paridade, dparidade) `Position` na coluna. Se a `Position` coluna for exibida `shared`, a unidade será compartilhada: Se for um disco rígido, será um disco particionado; se for um SSD, ele fará parte de um pool de armazenamento.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                 Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11      0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                 Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13      0   SSD        -  186.2GB  745.2GB (normal)
     shared   2.0.12      0   SSD        -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

Atribuir camadas locais (agregados) a VMs de storage (SVMs)

Se você atribuir uma ou mais camadas locais (agregados) a uma máquina virtual de storage (VM de storage ou SVM, anteriormente conhecido como SVM), você poderá usar apenas essas camadas locais para conter volumes para essa VM de storage (SVM).

O que você vai precisar

A VM de storage e os níveis locais que você deseja atribuir a essa VM de storage já devem existir.

Sobre esta tarefa

A atribuição de camadas locais às VMs de storage ajuda a manter as VMs de storage isoladas umas das outras. Isso é especialmente importante em um ambiente de alocação a vários clientes.

Passos

1. Confira a lista de camadas locais (agregados) já atribuídas ao SVM:

   ```
   vserver show -fields aggr-list
   ```

   Os agregados atualmente atribuídos à SVM são exibidos. Se não houver agregados atribuídos, é

apresentado "»-".

2. Adicione ou remova agregados atribuídos, dependendo dos seus requisitos:

Se você quiser…	Use este comando…
Atribuir agregados adicionais	`vserver add-aggregates`
Anular a atribuição de agregados	`vserver remove-aggregates`

Os agregados listados são atribuídos ou removidos do SVM. Se o SVM já tiver volumes que usam um agregado que não está atribuído ao SVM, uma mensagem de aviso será exibida, mas o comando será concluído com êxito. Todos os agregados que já foram atribuídos ao SVM e que não foram nomeados no comando não são afetados.

Exemplo

No exemplo a seguir, os agregados aggr1 e aggr2 são atribuídos ao SVM svm1:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

Determinar quais volumes residem em um nível local (agregado)

Talvez seja necessário determinar quais volumes residem em um nível local (agregado) antes de executar operações no nível local, como realocação ou desligamento.

Passos

1. Para exibir os volumes que residem em um agregado, insira

   ```
   volume show -aggregate aggregate_name
   ```

   Todos os volumes que residem no agregado especificado são exibidos.

Determinar e controlar o uso de espaço de um volume em um nível local (agregado)

Você pode determinar quais volumes do FlexVol estão usando mais espaço em um nível local (agregado) e, especificamente, quais recursos estão usando o volume.

O `volume show-footprint` comando fornece informações sobre o espaço físico de um volume ou sobre o uso do espaço dentro do agregado que contém.

O `volume show-footprint` comando mostra detalhes sobre o uso de espaço de cada volume em um agregado, incluindo volumes off-line. Este comando preenche a lacuna entre a saída `volume show-space` dos comandos e. `aggregate show-space` Todas as porcentagens são calculadas como uma porcentagem do tamanho agregado.

O exemplo a seguir mostra a `volume show-footprint` saída do comando para um volume chamado testvol:

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                                     Used    Used%
      --------------------------------    ----------    -----
      Volume Data Footprint                    120.6MB       4%
      Volume Guarantee                          1.88GB      71%
      Flexible Volume Metadata                 11.38MB       0%
      Delayed Frees                             1.36MB       0%
      Total Footprint                           2.01GB      76%
```

A tabela a seguir explica algumas das linhas-chave da saída do `volume show-footprint` comando e o que você pode fazer para tentar diminuir o uso do espaço por esse recurso:

Nome da linha/função	Descrição/conteúdo da linha	Algumas maneiras de diminuir
`Volume Data Footprint`	A quantidade total de espaço usada no agregado que contém os dados de um volume no sistema de arquivos ativo e o espaço usado pelas cópias Snapshot do volume. Esta linha não inclui espaço reservado.	• Eliminar dados do volume. • Exclusão de cópias Snapshot do volume.
`Volume Guarantee`	A quantidade de espaço reservado pelo volume no agregado para gravações futuras. A quantidade de espaço reservado depende do tipo de garantia do volume.	Alterar o tipo de garantia do volume para `none`.
`Flexible Volume Metadata`	A quantidade total de espaço usada no agregado pelos arquivos de metadados do volume.	Nenhum método direto para controlar.
`Delayed Frees`	Blocos que o ONTAP usou para desempenho e não podem ser liberados imediatamente. Para destinos SnapMirror, esta linha tem um valor de `0` e não é apresentada.	Nenhum método direto para controlar.
`File Operation Metadata`	A quantidade total de espaço reservado para metadados de operação de arquivo.	Nenhum método direto para controlar.

`Total Footprint`	A quantidade total de espaço que o volume usa no agregado. É a soma de todas as linhas.	Qualquer um dos métodos utilizados para diminuir o espaço utilizado por um volume.

Informações relacionadas

"Relatório técnico da NetApp 3483: Provisionamento reduzido em um ambiente empresarial SAN NetApp ou SAN IP"

Determinar o uso de espaço em um nível local (agregado)

É possível visualizar quanto espaço é usado por todos os volumes em uma ou mais camadas locais (agregados) para que você possa tomar medidas para liberar mais espaço.

O WAFL reserva uma porcentagem do espaço total em disco para metadados e performance de nível agregado. O espaço usado para manter os volumes no agregado sai da reserva WAFL e não pode ser alterado.

Em agregados menores que 30 TB, o WAFL reserva 10% do espaço total em disco para metadados e performance de nível agregado.

A partir do ONTAP 9.12,1, em agregados com 30 TB ou mais, a quantidade de espaço em disco reservado para metadados e performance de nível agregado é reduzida, resultando em 5% mais espaço utilizável em agregados. A disponibilidade dessa economia de espaço varia de acordo com sua plataforma e versão do ONTAP.

Espaço em disco reservado pela ONTAP em agregados 30 TB ou mais	Aplica-se a plataformas	Em versões ONTAP
5%	Todas as plataformas AFF e FAS	ONTAP 9.14,1 e posterior
5%	Plataformas AFF e plataformas FAS500f	ONTAP 9.12,1 e posterior
10%	Todas as plataformas	ONTAP 9.11,1 e posterior

É possível exibir o uso do espaço por todos os volumes em um ou mais agregados com o `aggregate show-space` comando. Isso ajuda você a ver quais volumes estão consumindo mais espaço em seus agregados contendo, para que você possa tomar ações para liberar mais espaço.

O espaço usado em um agregado é diretamente afetado pelo espaço usado nos volumes do FlexVol que ele contém. As medidas que você toma para aumentar o espaço em um volume também afetam o espaço no agregado.

> A partir do ONTAP 9.15,1, dois novos contadores de metadados estão disponíveis. Juntamente com as alterações em vários contadores existentes, você pode obter uma visão mais clara da quantidade de dados do usuário alocados. Consulte "Determinar o uso de espaço em um volume ou agregado" para obter mais informações.

As seguintes linhas estão incluídas na `aggregate show-space` saída do comando:

- **Pegadas de volume**

  O total de todas as pegadas de volume dentro do agregado. Ele inclui todo o espaço que é usado ou reservado por todos os dados e metadados de todos os volumes no agregado que contém.

- **Agregar metadados**

  Os metadados totais do sistema de arquivos exigidos pelo agregado, como bitmaps de alocação e arquivos de inode.

- **Reserva Snapshot**

  Quantidade de espaço reservado para cópias Snapshot agregadas, com base no tamanho do volume. Ele é considerado espaço usado e não está disponível para volume ou agregar dados ou metadados.

- **Reserva Snapshot inutilizável**

  A quantidade de espaço originalmente alocada para reserva Snapshot agregada que não está disponível para cópias Snapshot agregadas porque está sendo usada por volumes associados ao agregado. Só pode ocorrer em agregados com uma reserva de Snapshot de agregado que não seja zero.

- **Total utilizado**

  A soma de todo o espaço usado ou reservado no agregado por volumes, metadados ou cópias Snapshot.

- **Total físico utilizado**

  A quantidade de espaço que está sendo usada para dados agora (em vez de ser reservada para uso futuro). Inclui espaço usado por cópias Snapshot agregadas.

O exemplo a seguir mostra a `aggregate show-space` saída do comando para um agregado cuja reserva Snapshot é de 5%. Se a reserva de instantâneos for 0, a linha não será exibida.

```
cluster1::> storage aggregate show-space

                     Aggregate : wqa_gx106_aggr1

      Feature                                 Used      Used%
      --------------------------------    ----------     ------
      Volume Footprints                      101.0MB         0%
      Aggregate Metadata                       300KB         0%
      Snapshot Reserve                        5.98GB         5%

      Total Used                              6.07GB         5%
      Total Physical Used                    34.82KB         0%
```

Informações relacionadas

- "artigo da base de conhecimento: Uso do espaço"
- "Libere até 5% da sua capacidade de armazenamento atualizando para o ONTAP 9.12,1"

Realocar a propriedade de um nível local (agregado) dentro de um par de HA

É possível alterar a propriedade de camadas locais (agregados) entre os nós de um par de HA sem interromper o serviço das camadas locais.

Ambos os nós em um par de HA estão fisicamente conectados aos discos ou LUNs de array do outro. Cada LUN de disco ou array pertence a um dos nós.

A propriedade de todos os discos ou LUNs de array em um nível local (agregado) muda temporariamente de um nó para o outro quando ocorre um takeover. No entanto, as operações de realocação de camadas locais também podem alterar permanentemente a propriedade (por exemplo, se feito para balanceamento de carga). A propriedade muda sem processos de cópia de dados ou movimentação física dos discos ou LUNs de array.

Sobre esta tarefa

- Como os limites de contagem de volume são validados programaticamente durante as operações de realocação de nível local, não é necessário verificar isso manualmente.

  Se a contagem de volume exceder o limite suportado, a operação de realocação de nível local falhará com uma mensagem de erro relevante.

- Você não deve iniciar a realocação de nível local quando as operações no nível do sistema estiverem em andamento no nó de origem ou de destino. Da mesma forma, você não deve iniciar essas operações durante a realocação de nível local.

  Essas operações podem incluir o seguinte:

  - Takeover
  - Giveback
  - Encerramento
  - Outra operação de realocação de nível local
  - Alterações de propriedade do disco
  - Operações de configuração de volume ou camada local
  - Substituição do controlador de armazenamento
  - Atualização do ONTAP
  - Reversão do ONTAP
- Se você tiver uma configuração do MetroCluster, não deve iniciar a realocação de nível local enquanto as operações de recuperação de desastres (*switchover*, *curando* ou *switchback*) estiverem em andamento.
- Se você tiver uma configuração do MetroCluster e iniciar a realocação de nível local em um nível local comutado, a operação poderá falhar porque excederá a contagem de limite de volume do parceiro de DR.
- Você não deve iniciar a realocação de nível local em agregados que estejam corrompidos ou em manutenção.
- Antes de iniciar a realocação do nível local, você deve salvar todos os despejos principais nos nós de origem e destino.

Passos

1. Visualize os agregados no nó para confirmar quais agregados devem ser movidos e garantir que estejam on-line e em boas condições:

   `storage aggregate show -node` *`source-node`*

O comando a seguir mostra seis agregados nos quatro nós no cluster. Todos os agregados estão online. O node1 e o Node3 formam um par de HA e o Node2 e o Node4 formam um par de HA.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Emita o comando para iniciar a realocação agregada:

   `storage aggregate relocation start -aggregate-list` *`aggregate-1`*`,` *`aggregate-2`*`…`
   `-node` *`source-node`* `-destination` *`destination-node`*

   O comando a seguir move os agregados aggr_1 e aggr_2 de Node1 para Node3. Node3 é parceiro HA da Node1. Os agregados só podem ser movidos dentro do par de HA.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. Monitore o progresso da realocação agregada com o `storage aggregate relocation show` comando:

   `storage aggregate relocation show -node` *`source-node`*

   O comando a seguir mostra o progresso dos agregados que estão sendo movidos para Node3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

Quando a realocação estiver concluída, a saída deste comando mostra cada agregado com um status de relocação de "Concluído".

Excluir um nível local (agregado)

Você pode excluir um nível local (agregado) se não houver volumes no nível local.

`storage aggregate delete`O comando exclui um agregado de armazenamento. O comando falha se houver volumes presentes no agregado. Se o agregado tiver um armazenamento de objetos anexado a ele, além de excluir o agregado, o comando excluirá os objetos no armazenamento de objetos também. Nenhuma alteração é feita na configuração do armazenamento de objetos como parte deste comando.

O exemplo a seguir exclui um agregado chamado "aggr1":

```
> storage aggregate delete -aggregate aggr1
```

Comandos para realocação de agregados

Existem comandos ONTAP específicos para realocação de propriedade agregada em um par de HA.

Se você quiser…	Use este comando…
Inicie o processo de realocação de agregados	`storage aggregate relocation start`
Monitorar o processo de realocação de agregados	`storage aggregate relocation show`

Informações relacionadas

- "Referência do comando ONTAP"

Comandos para gerenciar agregados

Você usa o `storage aggregate` comando para gerenciar seus agregados.

Se você quiser…	Use este comando…
Exibir o tamanho do cache para todos os agregados Flash Pool	`storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total >0`
Exibir informações de disco e status de um agregado	`storage aggregate show-status`
Exibir discos sobressalentes por nó	`storage aggregate show-spare-disks`
Exibir os agregados de raiz no cluster	`storage aggregate show -has-mroot true`
Exibir informações básicas e status para agregados	`storage aggregate show`
Exibir o tipo de armazenamento usado em um agregado	`storage aggregate show -fields storage-type`
Traga um agregado on-line	`storage aggregate online`
Excluir um agregado	`storage aggregate delete`
Coloque um agregado no estado restrito	`storage aggregate restrict`
Renomeie um agregado	`storage aggregate rename`
Tire um agregado off-line	`storage aggregate offline`
Altere o tipo RAID de um agregado	`storage aggregate modify -raidtype`

Informações relacionadas

- "Referência do comando ONTAP"

Adicionar capacidade (discos) a um nível local (agregado)

Adicionar capacidade (discos) a um nível local (agregado)

Usando métodos diferentes, você segue um fluxo de trabalho específico para adicionar capacidade.

- "Fluxo de trabalho para adicionar capacidade a um nível local (agregado)"
- "Métodos para criar espaço em um nível local (agregado)"

É possível adicionar discos a uma camada local e adicionar unidades a um nó ou compartimento.

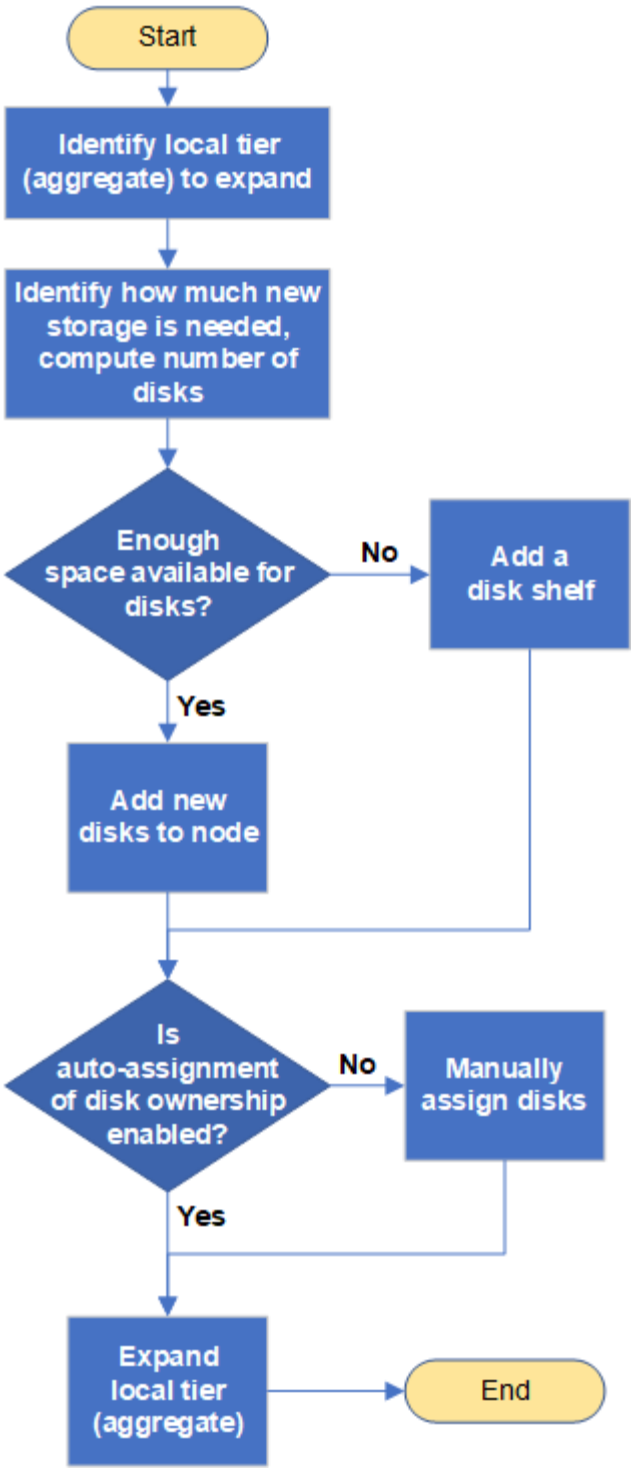
Se necessário, você pode corrigir partições sobressalentes desalinhadas.

- "Adicionar discos a um nível local (agregado)"
- "Adicionar unidades a um nó ou gaveta"
- "Corrija partições sobressalentes desalinhadas"

Fluxo de trabalho para adicionar capacidade a um nível local (expandindo um agregado)

Para adicionar capacidade a um nível local (expandir um agregado), primeiro você precisa identificar a camada local a que deseja adicionar, determinar a quantidade de storage novo necessário, instalar novos discos, atribuir propriedade de disco e criar um novo grupo RAID, se necessário.

Você pode usar o System Manager ou a CLI para adicionar capacidade.



Métodos para criar espaço em um nível local (agregado)

Se um nível local (agregado) ficar sem espaço livre, vários problemas podem resultar que vão desde a perda de dados até a desativação da garantia de um volume. Há várias maneiras de criar mais espaço em um nível local.

Todos os métodos têm várias consequências. Antes de tomar qualquer ação, você deve ler a seção relevante na documentação.

A seguir estão algumas maneiras comuns de fazer espaço no nível local, em ordem de menos para a maioria

das consequências:

- Adicione discos ao nível local.
- Mova alguns volumes para outro nível local com espaço disponível.
- Diminua o tamanho dos volumes com garantia de volume no nível local.
- Exclua cópias snapshot de volume desnecessárias se o tipo de garantia do volume for "'nenhum'".
- Eliminar volumes desnecessários.
- Habilite recursos de economia de espaço, como deduplicação ou compactação.
- (Temporariamente) desabilite recursos que estão usando uma grande quantidade de metadados .

Adicionar capacidade a um nível local (adicionar discos a um agregado)

É possível adicionar discos a um nível local (agregado) para que ele possa fornecer mais storage aos volumes associados.

Gerenciador de sistemas (ONTAP 9.8 e posterior)

Use o Gerenciador do sistema para adicionar capacidade (ONTAP 9.8 e posterior)

É possível adicionar capacidade a um nível local adicionando discos de capacidade.

A partir do ONTAP 9.12,1, você pode usar o Gerenciador de sistema para visualizar a capacidade comprometida de um nível local e determinar se a capacidade adicional é necessária para o nível local. "Monitorar a capacidade no System Manager"Consulte .

Sobre esta tarefa

Você só executa essa tarefa se tiver instalado o ONTAP 9.8 ou posterior. Se você instalou uma versão anterior do ONTAP, consulte a guia (ou seção) rotulada "Gerenciador do sistema (ONTAP 9.7 e anterior)".

Passos

1. Clique em **armazenamento > camadas**.
2. Clique ⋮ ao lado do nome do nível local ao qual você deseja adicionar capacidade.
3. Clique em **Adicionar capacidade**.

   Se não houver discos sobressalentes que você possa adicionar, a opção **Adicionar capacidade** não será exibida e você não poderá aumentar a capacidade do nível local.

4. Execute as seguintes etapas, com base na versão do ONTAP instalada:

Se esta versão do ONTAP estiver instalada…	Execute estas etapas…
ONTAP 9.8, 9,9 ou 9.10.1	a. Se o nó contiver várias camadas de storage, selecione o número de discos que deseja adicionar ao nível local. Caso contrário, se o nó contiver apenas uma camada de storage, a capacidade adicional será estimada automaticamente. b. Clique em **Add**.
Começando com ONTAP 9.11,1	a. Selecione o tipo de disco e o número de discos. b. Se quiser adicionar discos a um novo grupo RAID, marque a caixa de seleção. A alocação RAID é exibida. c. Clique em **Salvar**.

5. (Opcional) o processo leva algum tempo para ser concluído. Se quiser executar o processo em segundo plano, selecione **Executar em segundo plano**.
6. Depois que o processo for concluído, você poderá visualizar o aumento da capacidade nas informações do nível local em **Storage > Tiers**.

Gerenciador do sistema (ONTAP 9.7 e anteriores)

Use o Gerenciador do sistema para adicionar capacidade (ONTAP 9.7 e anterior)

Você pode adicionar capacidade a um nível local (agregado) adicionando discos de capacidade.

Sobre esta tarefa

Você só executa essa tarefa se tiver instalado o ONTAP 9.7 ou anterior. Se você instalou o ONTAP 9.8 ou posterior, Use o Gerenciador do sistema para adicionar capacidade (ONTAP 9.8 ou posterior)consulte .

Passos

1. (Apenas para o ONTAP 9.7) clique em **(retornar à versão clássica)**.
2. Clique em **hardware e diagnóstico > agregados**.
3. Selecione o agregado ao qual deseja adicionar discos de capacidade e clique em **ações > Adicionar capacidade**.

   Você deve adicionar discos com o mesmo tamanho que os outros discos no agregado.

4. (Apenas para ONTAP 9.7) clique em **mudar para a nova experiência**.
5. Clique em **armazenamento > camadas** para verificar o tamanho do novo agregado.

CLI

Use a CLI para adicionar capacidade

O procedimento para adicionar discos particionados a um agregado é semelhante ao procedimento para adicionar discos não particionados.

O que você vai precisar

Você deve saber qual é o tamanho do grupo RAID para o agregado ao qual está adicionando o armazenamento.

Sobre esta tarefa

Ao expandir um agregado, você deve estar ciente de se você está adicionando partição ou discos não particionados ao agregado. Quando você adiciona unidades não particionadas a um agregado existente, o tamanho dos grupos RAID existentes é herdado pelo novo grupo RAID, que pode afetar o número de discos de paridade necessários. Se um disco não particionado for adicionado a um grupo RAID composto por discos particionados, o novo disco será particionado, deixando uma partição sobressalente não utilizada.

Ao provisionar partições, você deve garantir que não saia do nó sem uma unidade com ambas as partições como sobressalente. Se o fizer, e o nó sofrer uma interrupção no controlador, informações valiosas sobre o problema (o arquivo principal) podem não estar disponíveis para fornecer ao suporte técnico.

Passos

1. Mostrar o armazenamento de reposição disponível no sistema que possui o agregado:

   `storage aggregate show-spare-disks -original-owner` *`node_name`*

   Você pode usar o `-is-disk-shared` parâmetro para mostrar apenas unidades particionadas ou apenas unidades não particionadas.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                     BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. Mostrar os grupos RAID atuais para o agregado:

   `storage aggregate show-status` *`aggr_name`*

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. Simule a adição do armazenamento ao agregado:

   `storage aggregate add-disks -aggregate` *`aggr_name`* `-diskcount` *`number_of_disks_or_partitions`* `-simulate true`

   Você pode ver o resultado da adição de storage sem realmente provisionar nenhum storage. Se algum aviso for exibido a partir do comando simulado, você pode ajustar o comando e repetir a simulação.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                        Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. Adicione o armazenamento ao agregado:

   `storage aggregate add-disks -aggregate` *`aggr_name`* `-raidgroup new -diskcount` *`number_of_disks_or_partitions`*

   Ao criar um agregado de Flash Pool, se você estiver adicionando discos com uma soma de verificação diferente do agregado ou se estiver adicionando discos a um agregado de checksum misto, você deverá usar o `-checksumstyle` parâmetro.

   Se você estiver adicionando discos a um agregado do Flash Pool, use o `-disktype` parâmetro para especificar o tipo de disco.

   Você pode usar o `-disksize` parâmetro para especificar um tamanho dos discos a serem adicionados. Somente os discos com aproximadamente o tamanho especificado são selecionados para adição ao agregado.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Verifique se o armazenamento foi adicionado com sucesso:

   `storage aggregate show-status -aggregate aggr_name`

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                                    Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                      0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                      0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                       0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Verifique se o nó ainda tem pelo menos uma unidade com a partição raiz e a partição de dados como sobressalente:

   `storage aggregate show-spare-disks -original-owner node_name`

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                     BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

Adicionar unidades a um nó ou gaveta

Você adiciona unidades a um nó ou gaveta para aumentar o número de hot spares ou para adicionar espaço à camada local (agregado).

Antes de começar

A unidade que você deseja adicionar deve ser suportada pela sua plataforma. Pode confirmar utilizando o "NetApp Hardware Universe".

O número mínimo de unidades que você deve adicionar em um único procedimento é seis. Adicionar uma única unidade pode reduzir o desempenho.

Passos para o NetApp Hardware Universe

1. No menu suspenso **Produtos**, selecione sua configuração de hardware
2. Selecione a sua plataforma.
3. Selecione a versão do ONTAP que você está executando e, em seguida, **Mostrar resultados**.
4. Abaixo do gráfico, selecione **clique aqui para ver vistas alternativas**. Escolha a exibição que corresponde à sua configuração.

Passos para instalar as unidades

1. Verifique "Site de suporte da NetApp"se há arquivos mais recentes do firmware da unidade e do compartimento e do Pacote de Qualificação de disco.

   Se o nó ou o compartimento não tiver as versões mais recentes, atualize-as antes de instalar a nova unidade.

   O firmware da unidade é atualizado automaticamente (sem interrupções) em novas unidades que não tenham versões de firmware atuais.

2. Aterre-se corretamente.
3. Retire cuidadosamente a moldura da parte frontal da plataforma.
4. Identifique a ranhura correta para a nova unidade.

   Os slots corretos para adicionar unidades variam dependendo do modelo da plataforma e da versão do ONTAP. Em alguns casos, você precisa adicionar unidades a slots específicos em sequência. Por exemplo, em um AFF A800, você adiciona as unidades em intervalos específicos, deixando clusters de slots vazios. Considerando que, em um AFF A220, você adiciona novas unidades aos próximos slots vazios, correndo do lado de fora para o meio da prateleira.

   Consulte as etapas em **antes de começar** para identificar os slots corretos para sua configuração no "NetApp Hardware Universe".

5. Insira a nova unidade:
   a. Com o manípulo do excêntrico na posição aberta, utilize as duas mãos para introduzir a nova transmissão.
   b. Prima até a unidade parar.
   c. Feche a pega do came de forma a que a unidade fique totalmente assente no plano intermédio e a pega encaixe no devido lugar. Certifique-se de que fecha lentamente a pega do excêntrico de forma a que fique corretamente alinhada com a face da unidade.
6. Verifique se o LED de atividade da unidade (verde) está aceso.

   Quando o LED de atividade da unidade está sólido, significa que a unidade tem energia. Quando o LED de atividade da unidade está intermitente, significa que a unidade tem alimentação e e/S está em curso. Se o firmware da unidade estiver sendo atualizado automaticamente, o LED pisca.

7. Para adicionar outra unidade, repita os passos 4 a 6.

   As novas unidades não são reconhecidas até que sejam atribuídas a um nó. Você pode atribuir as novas unidades manualmente ou esperar que o ONTAP atribua automaticamente as novas unidades se o nó seguir as regras para atribuição automática de unidade.

8. Depois de todas as novas unidades terem sido reconhecidas, verifique se foram adicionadas e se a sua propriedade está especificada corretamente.

Passos para confirmar a instalação

1. Exibir a lista de discos:

   ```
   storage aggregate show-spare-disks
   ```

   Você deve ver as novas unidades, de propriedade do nó correto.

2. **Opcionalmente (apenas para ONTAP 9.3 e versões anteriores),** zero as unidades recém-adicionadas:

   ```
   storage disk zerospares
   ```

   As unidades que foram usadas anteriormente em um nível local (agregado) do ONTAP devem ser zeradas antes que possam ser adicionadas a outro agregado. No ONTAP 9.3 e anterior, a restauração pode levar horas para ser concluída, dependendo do tamanho das unidades não zeradas no nó. A restauração das unidades agora pode evitar atrasos no caso de você precisar aumentar rapidamente o tamanho de uma camada local. Este não é um problema no ONTAP 9.4 ou posterior em que as unidades são zeradas usando *fast zero*, que leva apenas segundos.

Resultados

As novas unidades estão prontas. Você pode adicioná-los a um nível local (agregado), colocá-los na lista de hot spares ou adicioná-los ao criar um novo nível local.

Corrija partições sobressalentes desalinhadas

Quando você adiciona discos particionados a um nível local (agregado), você deve deixar um disco com a partição raiz e de dados disponível como um sobressalente para cada nó. Se você não tiver e seu nó sofrer uma interrupção, o ONTAP não poderá despejar o núcleo para a partição de dados sobressalente.

Antes de começar

Você deve ter uma partição de dados sobressalente e uma partição raiz sobressalente no mesmo tipo de disco de propriedade do mesmo nó.

Passos

1. Usando a CLI, exiba as partições sobressalentes para o nó:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Observe qual disco tem uma partição de dados sobressalente (spare_data) e qual disco tem uma partição raiz sobressalente (spare_root). A partição sobressalente mostrará um valor diferente de zero na `Local Data Usable` coluna ou `Local Root Usable`.

2. Substitua o disco por uma partição de dados sobressalente pelo disco pela partição raiz sobressalente:

   ```
   storage disk replace -disk spare_data -replacement spare_root -action start
   ```

   Você pode copiar os dados em qualquer direção; no entanto, copiar a partição raiz leva menos tempo para ser concluída.

3. Monitorize o progresso da substituição do disco:

   `storage aggregate show-status -aggregate aggr_name`

4. Após a conclusão da operação de substituição, exiba as peças sobressalentes novamente para confirmar que você tem um disco sobressalente completo:

   `storage aggregate show-spare-disks -original-owner node_name`

   Você deve ver um disco sobressalente com espaço utilizável sob "'local Data usable'" e `Local Root Usable`.

Exemplo

Você exibe suas partições sobressalentes para o nó C1-01 e vê que suas partições sobressalentes não estão alinhadas:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- ------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block         0B 73.89GB  828.0GB
```

Inicia o trabalho de substituição do disco:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

Enquanto aguarda a conclusão da operação de substituição, apresenta o progresso da operação:

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                     Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

Após a conclusão da operação de substituição, confirme se tem um disco sobressalente completo:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type    RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

Gerenciar discos

Visão geral do gerenciamento de discos

Você pode executar vários procedimentos para gerenciar discos em seu sistema.

- **Aspectos de gerenciamento de discos**
  - "Quando for necessário atualizar o Pacote de Qualificação de disco"
  - "Como os discos hot spare funcionam"
  - "Como os avisos de reserva baixos podem ajudá-lo a gerenciar seus discos sobressalentes"
  - "Opções adicionais de gerenciamento de particionamento de root-data"
- **Propriedade de disco e partição**
  - "Propriedade de disco e partição"

- * Falha na remoção do disco*
  - "Remover um disco com falha"
- **Sanitização de disco**
  - "Sanitização de disco"

Como os discos hot spare funcionam

Um disco hot spare é um disco que é atribuído a um sistema de armazenamento e está pronto para uso, mas não está em uso por um grupo RAID e não armazena nenhum dado.

Se ocorrer uma falha de disco em um grupo RAID, o disco hot spare é automaticamente atribuído ao grupo RAID para substituir os discos com falha. Os dados do disco com falha são reconstruídos no disco de substituição hot spare em segundo plano a partir do disco de paridade RAID. A atividade de reconstrução é registada no `/etc/message` ficheiro e é enviada uma mensagem AutoSupport.

Se o disco hot spare disponível não tiver o mesmo tamanho do disco com falha, um disco do tamanho maior seguinte é escolhido e depois reduzido para corresponder ao tamanho do disco que está substituindo.

Requisitos de substituição para disco transportador de vários discos

Manter o número adequado de peças sobressalentes para discos em suportes de vários discos é fundamental para otimizar a redundância de armazenamento e minimizar o tempo que o ONTAP deve gastar copiando discos para obter um layout de disco ideal.

Você precisa manter um mínimo de dois hot spares para discos de portadora de vários discos em todos os momentos. Para dar suporte ao uso do Centro de Manutenção e evitar problemas causados por várias falhas simultâneas de disco, você deve manter pelo menos quatro hot spares para operação em estado estável e substituir discos com falha imediatamente.

Se dois discos falharem ao mesmo tempo com apenas duas hot spares disponíveis, o ONTAP pode não ser capaz de trocar o conteúdo do disco com falha e seu companheiro de operadora para os discos sobressalentes. Esse cenário é chamado de impasse. Se isso acontecer, você será notificado através de mensagens EMS e mensagens AutoSupport. Quando as transportadoras de substituição estiverem disponíveis, tem de seguir as instruções fornecidas pelas mensagens EMS. Para obter informações, consulte o artigo da base de dados de Conhecimento "O layout RAID não pode ser corrigido automaticamente - mensagem AutoSupport"

Como os avisos de reserva baixos podem ajudá-lo a gerenciar seus discos sobressalentes

Por padrão, os avisos são emitidos para o console e logs se você tiver menos de uma unidade hot spare que corresponda aos atributos de cada unidade no sistema de armazenamento.

Você pode alterar o valor limite dessas mensagens de aviso para garantir que seu sistema siga as práticas recomendadas.

Sobre esta tarefa

Você deve definir a opção RAID "min_spare_count" como ""2"" para garantir que você sempre tenha o número mínimo recomendado de discos sobressalentes.

Passo

1. Defina a opção como "'2"":

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

Opções adicionais de gerenciamento de particionamento de root-data

A partir do ONTAP 9.2, uma nova opção de particionamento de dados raiz está disponível a partir do Menu de arranque, que fornece funcionalidades de gestão adicionais para discos configurados para particionamento de dados raiz.

Os seguintes recursos de gerenciamento estão disponíveis na opção Boot Menu (Menu de inicialização) 9.

- **Desparticionar todos os discos e remover suas informações de propriedade**

  Esta opção é útil se o seu sistema estiver configurado para o particionamento de dados root e você precisar reinicializá-lo com uma configuração diferente.

- **Limpe a configuração e inicialize o nó com discos particionados**

  Esta opção é útil para o seguinte:

  - Seu sistema não está configurado para particionamento de dados raiz e você gostaria de configurá-lo para particionamento de dados raiz
  - Seu sistema está configurado incorretamente para particionamento de dados raiz e você precisa corrigi-lo
  - Você tem uma plataforma AFF ou uma plataforma FAS com apenas SSDs conectados que está configurada para a versão anterior do particionamento de dados raiz e deseja atualizá-la para a versão mais recente do particionamento de dados raiz para obter maior eficiência de storage

- **Limpe a configuração e inicialize o nó com discos inteiros**

  Esta opção é útil se você precisar:

  - Desparticionar partições existentes
  - Remova a propriedade do disco local
  - Reinicialize seu sistema com discos inteiros usando RAID-DP

Quando for necessário atualizar o Pacote de Qualificação de disco

O Pacote de Qualificação de disco (DQP) adiciona suporte completo para unidades recém-qualificadas. Antes de atualizar o firmware da unidade ou adicionar novos tipos ou tamanhos de unidade a um cluster, é necessário atualizar o DQP. Uma prática recomendada é também atualizar o DQP regularmente; por exemplo, a cada trimestre ou semestralmente.

Você precisa baixar e instalar o DQP nas seguintes situações:

- Sempre que você adicionar um novo tipo ou tamanho de unidade ao nó

  Por exemplo, se você já tiver unidades de 1 TB e adicionar unidades de 2 TB, precisará verificar a atualização DQP mais recente.

- Sempre que atualizar o firmware do disco
- Sempre que estiverem disponíveis ficheiros DQP ou firmware de disco mais recentes
- Sempre que você atualizar para uma nova versão do ONTAP.

  O DQP não é atualizado como parte de uma atualização do ONTAP.

Informações relacionadas

"NetApp Downloads: Pacote de Qualificação de disco"

"Downloads do NetApp: Firmware da unidade de disco"

Propriedade de disco e partição

Propriedade de disco e partição

Você pode gerenciar a propriedade de discos e partições.

Você pode executar as seguintes tarefas:

- **"Exibir a propriedade do disco e da partição"**

  Você pode exibir a propriedade do disco para determinar qual nó controla o armazenamento. Você também pode exibir a propriedade da partição em sistemas que usam discos compartilhados.

- **"Altere as configurações para atribuição automática de propriedade de disco"**

  Você pode selecionar uma política não padrão para atribuir automaticamente a propriedade do disco ou desativar a atribuição automática da propriedade do disco.

- **"Atribua manualmente a propriedade de discos não particionados"**

  Se o cluster não estiver configurado para usar atribuição automática de propriedade de disco, você deverá atribuir propriedade manualmente.

- **"Atribua manualmente a propriedade de discos particionados"**

  Você pode definir a propriedade do disco do contentor ou as partições manualmente ou usando atribuição automática - assim como você faz para discos não particionados.

- **"Remover um disco com falha"**

  Um disco que falhou completamente não é mais considerado pelo ONTAP como um disco utilizável, e você pode desconetar imediatamente o disco da gaveta.

- **"Remova a propriedade de um disco"**

  O ONTAP grava informações de propriedade do disco no disco. Antes de remover um disco sobressalente ou seu compartimento de um nó, remova as informações de propriedade para que ele possa ser devidamente integrado a outro nó.

Sobre a atribuição automática de propriedade de disco

A atribuição automática de discos não possuídos é ativada por padrão. As atribuições de

propriedade automática de disco ocorrem 10 minutos após a inicialização do par de HA e a cada cinco minutos durante a operação normal do sistema.

Quando você adiciona um novo disco a um par de HA, por exemplo, ao substituir um disco com falha, ao responder a uma mensagem de "peças sobressalentes baixas" ou à adição de capacidade, a política de atribuição automática padrão atribui a propriedade do disco a um nó como sobressalente.

A política de atribuição automática padrão é baseada em características específicas da plataforma ou no compartimento DS460C se o seu par de HA tiver apenas essas gavetas e usar um dos seguintes métodos (políticas) para atribuir a propriedade do disco:

Método de atribuição	Efeito nas atribuições de nós	Configurações de plataforma que padrão para o método de atribuição
baía	Baias de números pares são atribuídas ao nó A e baias de números ímpares ao nó B.	Sistemas de nível de entrada em uma configuração de par de HA com um único compartimento compartilhado.
gaveta	Todos os discos na gaveta são atribuídos ao nó A.	Sistemas de nível básico em uma configuração de par de HA com uma stack de duas ou mais gavetas e configurações de MetroCluster com uma stack por nó, duas ou mais gavetas.
prateleira dividida Esta política está sob o valor "defeito" para o `-autoassign -policy` parâmetro `storage disk option` do comando para configurações de plataforma e prateleira aplicáveis.	Os discos no lado esquerdo da gaveta são atribuídos ao nó A e do lado direito ao nó B. as gavetas parciais em pares de HA são enviadas de fábrica com discos preenchidos da borda do compartimento em direção ao centro.	A maioria das plataformas AFF e algumas configurações do MetroCluster.
pilha	Todos os discos na pilha são atribuídos ao nó A.	Sistemas de nível de entrada independentes e todas as outras configurações.

meia gaveta Esta política está sob o valor "defeito" para o `-autoassign -policy` parâmetro `storage disk option` do comando para configurações de plataforma e prateleira aplicáveis.	Todas as unidades na metade esquerda de uma gaveta DS460C (compartimentos de unidades 0 a 5) são atribuídas ao nó A; todas as unidades na metade direita de uma gaveta (compartimentos de unidades 6 a 11) são atribuídas ao nó B. Ao inicializar um par de HA com apenas DS460C gavetas, a atribuição automática de propriedade de disco não é suportada. Você deve atribuir manualmente a propriedade para unidades que contêm unidades raiz/contentor que têm a partição raiz, de acordo com a política de meia gaveta.	Pares DE HA com apenas DS460C gavetas, após a inicialização do par de HA (inicialização). Depois que um par de HA é inicializado, a atribuição automática de propriedade de disco é ativada automaticamente e usa a política de meia gaveta para atribuir propriedade às unidades restantes (exceto as unidades raiz/unidades de contentor que têm a partição raiz) e quaisquer unidades adicionadas no futuro. Se o seu par de HA tiver DS460C gavetas além de outros modelos de gaveta, a política de meia gaveta não será usada. A política padrão usada é ditada por caraterísticas específicas da plataforma.

Definições e modificações de atribuição automática:

- Pode apresentar as definições de atribuição automática atuais (ligado/desligado) com o `storage disk option show` comando.
- Você pode desativar a atribuição automática usando o `storage disk option modify` comando.
- Se a política de atribuição automática padrão não for desejável em seu ambiente, você poderá especificar (alterar) o método de atribuição de compartimento, compartimento ou pilha usando o `-autoassign -policy` parâmetro no `storage disk option modify` comando.

  Aprenda a "Altere as configurações para atribuição automática de propriedade de disco".

> As políticas de atribuição automática padrão de meia gaveta e prateleira dividida são exclusivas porque não podem ser definidas por usuários como as diretivas de compartimento, compartimento e pilha podem.

Em sistemas de particionamento avançado de unidade (ADP), para fazer com que a atribuição automática funcione em compartimentos com meia densidade, as unidades devem ser instaladas nos compartimentos de gaveta corretos com base no tipo de gaveta que você tem:

- Se a gaveta não for uma gaveta de DS460C TB, instale as unidades igualmente no lado esquerdo e no lado direito, movendo-se em direção ao meio. Por exemplo, seis unidades nos compartimentos 0-5 e seis unidades nos compartimentos 18-23 de uma gaveta de DS224C U.
- Se a gaveta for uma gaveta de DS460C TB, instale as unidades na linha da frente (compartimentos de unidades 0, 3, 6 e 9) de cada gaveta. Para as unidades restantes, distribua-as uniformemente em cada gaveta preenchendo as linhas da gaveta da frente para trás. Se você não tiver unidades suficientes para preencher linhas, instale-as em pares para que as unidades ocupem o lado esquerdo e direito de uma gaveta uniformemente.

A instalação de acionamentos na fila dianteira de cada gaveta permite um fluxo de ar adequado e evita o superaquecimento.

> Se as unidades não estiverem instaladas nos compartimentos de gaveta corretos nas gavetas com meia densidade, quando uma unidade de contêiner falhar e for substituída, o ONTAP não atribuirá propriedade automaticamente. Neste caso, a atribuição da nova unidade de contentor precisa ser feita manualmente. Depois de ter atribuído a propriedade para a unidade de contentor, o ONTAP manipula automaticamente todas as atribuições de particionamento e particionamento de unidades necessárias.

Em algumas situações em que a atribuição automática não funcionará, você precisa atribuir manualmente a propriedade do disco usando o `storage disk assign` comando:

- Se você desativar a atribuição automática, os novos discos não estarão disponíveis como sobressalentes até que sejam atribuídos manualmente a um nó.
- Se você quiser que os discos sejam atribuídos automaticamente e tiver várias pilhas ou gavetas que precisam ter propriedade diferente, um disco deve ter sido atribuído manualmente em cada pilha ou compartimento para que a atribuição automática de propriedade funcione em cada pilha ou compartimento.
- Se a atribuição automática estiver ativada e você atribuir manualmente uma única unidade a um nó que não esteja especificado na política ativa, a atribuição automática pára de funcionar e uma mensagem EMS será exibida.

Aprenda a "Atribua manualmente a propriedade do disco de discos não particionados".

Aprenda a "Atribua manualmente a propriedade do disco de discos particionados".

Exibir a propriedade do disco e da partição

Você pode exibir a propriedade do disco para determinar qual nó controla o armazenamento. Você também pode exibir a propriedade da partição em sistemas que usam discos compartilhados.

Passos

1. Exibir a propriedade de discos físicos:

   ```
   storage disk show -ownership
   ```

```
cluster::> storage disk show -ownership
Disk     Aggregate Home     Owner    DR Home  Home ID     Owner ID   DR
Home ID  Reserver    Pool
-------- --------- -------- -------- -------- ---------- -----------
----------- ----------- ------
1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
1.0.3    -         node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
```

2. Se você tiver um sistema que usa discos compartilhados, poderá exibir a propriedade da partição:

   `storage disk show -partition-ownership`

```
cluster::> storage disk show -partition-ownership
                                Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

Altere as configurações para atribuição automática de propriedade de disco

Você pode usar o `storage disk option modify` comando para selecionar uma política não padrão para atribuir automaticamente a propriedade do disco ou para desativar a atribuição automática de propriedade do disco.

Saiba mais "atribuição automática da propriedade do disco"sobre .

Sobre esta tarefa

Se você tiver um par de HA com apenas DS460C gavetas, a política de atribuição automática padrão será de meia gaveta. Não é possível alterar para uma política não padrão (compartimento, compartimento, pilha).

Passos

1. Modificar atribuição automática de disco:
   a. Se pretender selecionar uma política não predefinida, introduza:

      `storage disk option modify -autoassign-policy *autoassign_policy* -node *node_name*`

      - `stack`Use como o `*autoassign_policy*` para configurar a propriedade automática no nível de pilha ou loop.
      - `shelf`Use como o `*autoassign_policy*` para configurar a propriedade automática no nível do compartimento.
      - `bay`Utilize como o `*autoassign_policy*` para configurar a propriedade automática no nível do compartimento.

   b. Se pretender desativar a atribuição automática de propriedade de disco, introduza:

      `storage disk option modify -autoassign off -node *node_name*`

2. Verifique as configurações de atribuição automática dos discos:

   `storage disk option show`

```
cluster1::> storage disk option show

Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                          Assign Policy
-------------  -------------  ------------  -------------  --------
cluster1-1     on             on            on             default
cluster1-2     on             on            on             default
```

Atribua manualmente a propriedade do disco de discos não particionados

Se o seu par de HA não estiver configurado para usar a atribuição automática de propriedade de disco, você deverá atribuir manualmente a propriedade. Se você estiver inicializando um par de HA que tenha apenas DS460C gavetas, será necessário atribuir manualmente a propriedade das unidades raiz.

Sobre esta tarefa

- Se você estiver atribuindo manualmente a propriedade de um par de HA que não está sendo inicializado e não tiver apenas DS460C gavetas, use a opção 1.
- Se você estiver inicializando um par de HA com apenas DS460C gavetas, use a opção 2 para atribuir manualmente a propriedade para as unidades raiz.

Opção 1: Maioria dos pares de HA

Para um par de HA que não está sendo inicializado e não tem apenas DS460C gavetas, use este procedimento para atribuir manualmente a propriedade.

Sobre esta tarefa

- Os discos para os quais você está atribuindo propriedade devem estar em uma gaveta que esteja fisicamente cabeada para o nó ao qual você está atribuindo propriedade.
- Se você estiver usando discos em um nível local (agregado):
  - Os discos devem ser de propriedade de um nó antes que possam ser usados em um nível local (agregado).
  - Não é possível reatribuir a propriedade de um disco que esteja em uso em um nível local (agregado).

Passos

1. Use a CLI para exibir todos os discos não possuídos:

   ```
   storage disk show -container-type unassigned
   ```

2. Atribuir cada disco:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   Você pode usar o caractere curinga para atribuir mais de um disco de uma vez. Se você estiver reatribuindo um disco sobressalente que já é de propriedade de um nó diferente, você deve usar a opção "'-force".

Opção 2: Um par de HA com apenas DS460C gavetas

Para um par de HA que você está inicializando e que tenha apenas DS460C gavetas, use este procedimento para atribuir manualmente a propriedade das unidades raiz.

Sobre esta tarefa

- Ao inicializar um par de HA que tenha apenas DS460C gavetas, você deve atribuir manualmente as unidades raiz para estar em conformidade com a política de meia gaveta.

  Após a inicialização do par de HA (inicialização), a atribuição automática da propriedade do disco é ativada automaticamente e usa a política de meia gaveta para atribuir propriedade às unidades restantes (exceto as unidades raiz) e a quaisquer unidades adicionadas no futuro, como a substituição de discos com falha, a resposta a uma mensagem de "peças sobressalentes baixas" ou a adição de capacidade.

  Saiba mais sobre a política de meia gaveta no "Sobre a atribuição automática de propriedade de disco"tópico .

- O RAID precisa de um mínimo de 10 unidades para cada par de HA (5 TB para cada nó) para quaisquer unidades NL-SAS superiores a 8TB TB em uma gaveta de DS460C TB.

Passos

1. Se as DS460C gavetas não estiverem totalmente preenchidas, execute as seguintes etapas; caso contrário, vá para a próxima etapa.

   a. Primeiro, instale unidades na linha dianteira (compartimentos de unidades 0, 3, 6 e 9) de cada gaveta.

      A instalação de acionamentos na fila dianteira de cada gaveta permite um fluxo de ar adequado e evita o superaquecimento.

   b. Para as unidades restantes, distribua-as uniformemente em cada gaveta.

      Encha as linhas da gaveta da frente para trás. Se você não tiver unidades suficientes para preencher linhas, instale-as em pares para que as unidades ocupem o lado esquerdo e direito de uma gaveta uniformemente.

      A ilustração a seguir mostra a numeração do compartimento de unidades e os locais em uma gaveta DS460C.

2. Faça login no clustershell usando o LIF de gerenciamento de nó ou LIF de gerenciamento de cluster.
3. Atribua manualmente as unidades raiz em cada gaveta para estar em conformidade com a política de meia gaveta usando as seguintes subetapas:

   A política de meia gaveta atribui a metade esquerda das unidades de uma gaveta (compartimentos 0 a 5) ao nó A e a metade direita das unidades de uma gaveta (compartimentos 6 a 11) ao nó B.

   a. Exibir todos os discos não possuídos:
   `storage disk show -container-type unassigned`
   b. Atribuir os discos raiz:
   `storage disk assign -disk disk_name -owner owner_name`

      Você pode usar o caractere curinga para atribuir mais de um disco de cada vez.

Atribua manualmente a propriedade de discos particionados

Você pode atribuir manualmente a propriedade do disco de contentor ou as partições em sistemas de particionamento de unidade avançado (ADP). Se você estiver inicializando um par de HA que tenha apenas DS460C gavetas, será necessário atribuir manualmente a propriedade para as unidades de contentor que incluirão partições raiz.

Sobre esta tarefa

- O tipo de sistema de armazenamento que você determina qual método de ADP é suportado, dados de raiz (RD) ou dados-raiz (RD2).

  Os sistemas de storage FAS usam RD e os sistemas de storage AFF usam RD2.

- Se você estiver atribuindo manualmente propriedade em um par de HA que não está sendo inicializado e não tem apenas DS460C gavetas, use a opção 1 para atribuir manualmente discos com particionamento de dados raiz (RD) ou use a opção 2 para atribuir manualmente discos com particionamento de dados raiz (RD2).
- Se você estiver inicializando um par de HA com apenas DS460C gavetas, use a opção 3 para atribuir

manualmente a propriedade para as unidades de contentor que têm a partição raiz.

Opção 1: Atribuir manualmente discos com particionamento de dados raiz (RD)

Para o particionamento de dados raiz, existem três entidades de propriedade (o disco de contentor e as duas partições) coletivamente propriedade do par HA.

Sobre esta tarefa

- O disco de contêiner e as duas partições nem todas precisam ser de propriedade do mesmo nó no par de HA, contanto que todas sejam de propriedade de um dos nós do par de HA. No entanto, quando você usa uma partição em um nível local (agregado), ela deve ser de propriedade do mesmo nó que possui o nível local.
- Se um disco de contentor falhar em um compartimento com meio preenchimento e for substituído, talvez seja necessário atribuir manualmente a propriedade do disco porque o ONTAP nem sempre atribui propriedade automaticamente nesse caso.
- Depois que o disco de contentor é atribuído, o software do ONTAP manipula automaticamente todas as atribuições de particionamento e partição necessárias.

Passos

1. Use a CLI para exibir a propriedade atual do disco particionado:

   `storage disk show -disk disk_name -partition-ownership`

2. Defina o nível de privilégio CLI como avançado:

   `set -privilege advanced`

3. Digite o comando apropriado, dependendo da entidade de propriedade para a qual você deseja atribuir propriedade:

   Se alguma das entidades de propriedade já for detida, deverá incluir a opção ""-force".

Se pretender atribuir propriedade para a…	Use este comando…
Disco do contêiner	`storage disk assign -disk disk_name -owner owner_name`
Partição de dados	`storage disk assign -disk disk_name -owner owner_name -data true`
Partição raiz	`storage disk assign -disk disk_name -owner owner_name -root true`

Opção 2: Atribuir manualmente discos com particionamento root-data-data (RD2)

Para o particionamento de dados-raiz, existem quatro entidades de propriedade (o disco do contentor e as três partições) coletivamente propriedade do par HA. O particionamento root-data-data cria uma pequena partição como a partição raiz e duas partições maiores e igualmente dimensionadas para dados.

Sobre esta tarefa

- Os parâmetros devem ser usados com o `disk assign` comando para atribuir a partição adequada de um disco particionado root-data-data-data. Você não pode usar esses parâmetros com discos que fazem parte de um pool de armazenamento. O valor padrão é "false".
  - O `-data1 true` parâmetro atribui a partição "d.ATA1" de um disco particionado root-data1-data2.
  - O `-data2 true` parâmetro atribui a partição "d.ata2" de um disco particionado root-data1-data2.
- Se um disco de contentor falhar em um compartimento com meio preenchimento e for substituído, talvez seja necessário atribuir manualmente a propriedade do disco porque o ONTAP nem sempre atribui propriedade automaticamente nesse caso.
- Depois que o disco de contentor é atribuído, o software do ONTAP manipula automaticamente todas as atribuições de particionamento e partição necessárias.

Passos

1. Use a CLI para exibir a propriedade atual do disco particionado:

   `storage disk show -disk disk_name -partition-ownership`

2. Defina o nível de privilégio CLI como avançado:

   `set -privilege advanced`

3. Digite o comando apropriado, dependendo da entidade de propriedade para a qual você deseja atribuir propriedade:

   Se alguma das entidades de propriedade já for detida, deverá incluir a opção ""-force".

Se pretender atribuir propriedade para a…	Use este comando…
Disco do contêiner	`storage disk assign -disk disk_name -owner owner_name`
Data1 partição	`storage disk assign -disk disk_name -owner owner_name -data1 true`
Data2 partição	`storage disk assign -disk disk_name -owner owner_name -data2 true`
Partição raiz	`storage disk assign -disk disk_name -owner owner_name -root true`

Opção 3: Atribua manualmente unidades de contentor DS460C que tenham a partição raiz

Se você estiver inicializando um par de HA que tenha apenas DS460C gavetas, será necessário atribuir manualmente a propriedade para as unidades de contêiner que têm a partição raiz, de acordo com a política de meia gaveta.

Sobre esta tarefa

- Quando você inicializar um par de HA que tenha apenas DS460C gavetas, as opções 9a e 9b do menu de inicialização ADP (disponível com o ONTAP 9.2 e posteriores) não suportam a atribuição automática de propriedade da unidade. Você deve atribuir manualmente as unidades de contentor que têm a partição raiz, de acordo com a política de meia gaveta.

  Após a inicialização do par de HA (inicialização), a atribuição automática da propriedade do disco é ativada automaticamente e usa a política de meia gaveta para atribuir propriedade às unidades restantes (exceto as unidades de contentor que têm a partição raiz) e quaisquer unidades adicionadas no futuro, como a substituição de unidades com falha, a resposta a uma mensagem de "peças sobressalentes baixas" ou a adição de capacidade.

- Saiba mais sobre a política de meia gaveta no "Sobre a atribuição automática de propriedade de disco"tópico .

Passos

1. Se as DS460C gavetas não estiverem totalmente preenchidas, execute as seguintes etapas; caso contrário, vá para a próxima etapa.

   a. Primeiro, instale unidades na linha dianteira (compartimentos de unidades 0, 3, 6 e 9) de cada gaveta.

      A instalação de acionamentos na fila dianteira de cada gaveta permite um fluxo de ar adequado e evita o superaquecimento.

   b. Para as unidades restantes, distribua-as uniformemente em cada gaveta.

      Encha as linhas da gaveta da frente para trás. Se você não tiver unidades suficientes para preencher linhas, instale-as em pares para que as unidades ocupem o lado esquerdo e direito de uma gaveta uniformemente.

      A ilustração a seguir mostra a numeração do compartimento de unidades e os locais em uma gaveta DS460C.

2. Faça login no clustershell usando o LIF de gerenciamento de nó ou LIF de gerenciamento de cluster.
3. Para cada gaveta, atribua manualmente as unidades de contentor que têm a partição raiz, de acordo com a política de meia gaveta usando as seguintes subetapas:

   A política de meia gaveta atribui a metade esquerda das unidades de uma gaveta (compartimentos 0 a 5) ao nó A e a metade direita das unidades de uma gaveta (compartimentos 6 a 11) ao nó B.

   a. Exibir todos os discos não possuídos:
   `storage disk show -container-type unassigned`

   b. Atribua as unidades de contentor que têm a partição raiz:
   `storage disk assign -disk disk_name -owner owner_name`

   Você pode usar o caractere curinga para atribuir mais de uma unidade de cada vez.

Configure uma configuração ativo-passivo em nós usando o particionamento root-data

Quando um par de HA é configurado para usar o particionamento de dados raiz pela fábrica, a propriedade das partições de dados é dividida entre ambos os nós do par para uso em uma configuração ativo-ativo. Se você quiser usar o par de HA em uma configuração ativo-passivo, é necessário atualizar a propriedade da partição antes de criar seu nível local de dados (agregado).

O que você vai precisar

- Você deve ter decidido qual nó será o nó ativo e qual nó será o nó passivo.
- O failover de storage deve ser configurado no par de HA.

Sobre esta tarefa

Esta tarefa é executada em dois nós: Nó A e nó B.

Este procedimento foi projetado para nós para os quais nenhum nível local de dados (agregado) foi criado a partir dos discos particionados.

Saiba mais "particionamento avançado de disco"sobre .

Passos

Todos os comandos são inseridos no shell do cluster.

1. Veja a propriedade atual das partições de dados:

   ```
   storage aggregate show-spare-disks
   ```

   A saída mostra que metade das partições de dados são propriedade de um nó e metade são propriedade do outro nó. Todas as partições de dados devem ser sobressalentes.

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
```

```
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. Introduza o nível de privilégio avançado:

   ```
   set advanced
   ```

3. Para cada partição de dados pertencente ao nó que será o nó passivo, atribua-o ao nó ativo:

   ```
   storage disk assign -force -data true -owner active_node_name -disk disk_name
   ```

   Não é necessário incluir a partição como parte do nome do disco.

   Você digitaria um comando semelhante ao exemplo a seguir para cada partição de dados que você precisa reatribuir:

   ```
   storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
   ```

4. Confirme se todas as partições estão atribuídas ao nó ativo.

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                              Local
Local
                                                               Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
```

```
 1.0.1                        BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                       BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                        BSAS    7200 block               0B
73.89GB  828.0GB
13 entries were displayed.
```

Note que cluster1-02 ainda possui uma partição raiz sobressalente.

5. Retornar ao privilégio administrativo:

   `set admin`

6. Crie seu agregado de dados, deixando pelo menos uma partição de dados como sobressalente:

   `storage aggregate create` *`new_aggr_name`* `-diskcount` *`number_of_partitions`* `-node`

active_node_name

O agregado de dados é criado e pertence ao nó ativo.

Configure uma configuração ativo-passivo em nós usando o particionamento root-data-data

Quando um par de HA é configurado para usar o particionamento de dados-raiz pela fábrica, a propriedade das partições de dados é dividida entre ambos os nós do par para uso em uma configuração ativo-ativo. Se você quiser usar o par de HA em uma configuração ativo-passivo, é necessário atualizar a propriedade da partição antes de criar seu nível local de dados (agregado).

O que você vai precisar

- Você deve ter decidido qual nó será o nó ativo e qual nó será o nó passivo.
- O failover de storage deve ser configurado no par de HA.

Sobre esta tarefa

Esta tarefa é executada em dois nós: Nó A e nó B.

Este procedimento foi projetado para nós para os quais nenhum nível local de dados (agregado) foi criado a partir dos discos particionados.

Saiba mais "particionamento avançado de disco"sobre .

Passos

Todos os comandos são inseridos no shell do cluster.

1. Veja a propriedade atual das partições de dados:

   `storage aggregate show-spare-disks -original-owner` *`passive_node_name`* `-fields local-usable-data1-size, local-usable-data2-size`

   A saída mostra que metade das partições de dados são propriedade de um nó e metade são propriedade do outro nó. Todas as partições de dados devem ser sobressalentes.

2. Introduza o nível de privilégio avançado:

   `set advanced`

3. Para cada partição data1 pertencente ao nó que será o nó passivo, atribua-o ao nó ativo:

   `storage disk assign -force -data1 -owner` *`active_node_name`* `-disk` *`disk_name`*

   Não é necessário incluir a partição como parte do nome do disco

4. Para cada partição data2 pertencente ao nó que será o nó passivo, atribua-o ao nó ativo:

   `storage disk assign -force -data2 -owner` *`active_node_name`* `-disk` *`disk_name`*

   Não é necessário incluir a partição como parte do nome do disco

5. Confirme se todas as partições estão atribuídas ao nó ativo:

storage aggregate show-spare-disks

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
```

```
Root Physical
 Disk                        Type      RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Note que cluster1-02 ainda possui uma partição raiz sobressalente.

6. Retornar ao privilégio administrativo:

   `set admin`

7. Crie seu agregado de dados, deixando pelo menos uma partição de dados como sobressalente:

   `storage aggregate create` *`new_aggr_name`* `-diskcount` *`number_of_partitions`* `-node` *`active_node_name`*

   O agregado de dados é criado e pertence ao nó ativo.

8. Como alternativa, você pode usar o layout agregado recomendado do ONTAP, que inclui as práticas recomendadas para o layout do grupo RAID e contagens de reserva:

   `storage aggregate auto-provision`

Remova a propriedade de um disco

O ONTAP grava informações de propriedade do disco no disco. Antes de remover um disco sobressalente ou seu compartimento de um nó, remova as informações de propriedade para que ele possa ser devidamente integrado a outro nó.

> Se o disco estiver particionado para o particionamento de dados raiz e estiver a executar o ONTAP 9.10,1 ou posterior, contacte o suporte técnico da NetApp para obter assistência na remoção de propriedade. Para obter mais informações, consulte "artigo da base de dados de conhecimento: Falha ao remover o proprietário do disco".

O que você vai precisar

O disco do qual você deseja remover a propriedade deve atender aos seguintes requisitos:

- Deve ser um disco sobressalente.

  Não é possível remover a propriedade de um disco que está sendo usado em um nível local (agregado).

- Não pode estar no centro de manutenção.
- Não pode estar em processo de sanitização.
- Não pode ter falhado.

  Não é necessário remover a propriedade de um disco com falha.

Sobre esta tarefa

Se a atribuição automática de disco estiver ativada, o ONTAP poderá reatribuir automaticamente a propriedade antes de remover o disco do nó. Por esse motivo, desative a atribuição automática de propriedade até que o disco seja removido e, em seguida, reative-o.

Passos

1. Se a atribuição automática de propriedade de disco estiver ativada, use a CLI para desativá-la:

   `storage disk option modify -node node_name -autoassign off`

2. Se necessário, repita a etapa anterior para o parceiro de HA do nó.
3. Remova as informações de propriedade do software do disco:

   `storage disk removeowner disk_name`

   Para remover informações de propriedade de vários discos, use uma lista separada por vírgulas.

   Exemplo:

   ```
   storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
   ```

4. Se o disco estiver particionado para o particionamento de dados raiz e você estiver executando o ONTAP 9.9,1 ou anterior, remova a propriedade das partições:

   `storage disk removeowner -disk disk_name -root true`

   `storage disk removeowner -disk disk_name -data true`

   Ambas as partições não são mais propriedade de nenhum nó.

5. Se você desativou anteriormente a atribuição automática da propriedade do disco, ative-o depois que o disco tiver sido removido ou reatribuído:

   `storage disk option modify -node node_name -autoassign on`

6. Se necessário, repita a etapa anterior para o parceiro de HA do nó.

Remover um disco com falha

Um disco que falhou completamente não é mais contado pelo ONTAP como um disco utilizável, e você pode desconetar imediatamente o disco do compartimento de disco. No entanto, você deve deixar um disco parcialmente com falha conetado por tempo suficiente para que o processo de recuperação RAID rápida seja concluído.

Sobre esta tarefa

Se você estiver removendo um disco porque ele falhou ou porque está produzindo mensagens de erro excessivas, você não deve usar o disco novamente neste ou em qualquer outro sistema de armazenamento.

Passos

1. Use a CLI para localizar a ID do disco com falha:

```
storage disk show -broken
```

Se o disco não aparecer na lista de discos com falha, ele pode ter parcialmente falhado, com uma recuperação RAID rápida em processo. Neste caso, você deve esperar até que o disco esteja presente na lista de discos com falha (o que significa que o processo de recuperação rápida de RAID está concluído) antes de remover o disco.

2. Determine a localização física do disco que você deseja remover:

```
storage disk set-led -action on -disk disk_name 2
```

O LED de avaria na face do disco está aceso.

3. Remova o disco do compartimento de disco, seguindo as instruções no guia de hardware do modelo do compartimento de disco.

Sanitização de disco

Visão geral da sanitização de disco

A sanitização de disco é o processo de obliteração física de dados, substituindo discos ou SSDs com padrões de bytes especificados ou dados aleatórios para que a recuperação dos dados originais se torne impossível. O uso do processo de sanitização garante que ninguém possa recuperar os dados nos discos.

Esta funcionalidade está disponível através do nodeshell em todas as versões do ONTAP 9, e começando com o ONTAP 9.6 no modo de manutenção.

O processo de sanitização de disco usa três padrões sucessivos de substituição de bytes padrão ou especificados pelo usuário para até sete ciclos por operação. O padrão de substituição aleatória é repetido para cada ciclo.

Dependendo da capacidade do disco, dos padrões e do número de ciclos, o processo pode levar várias horas. A sanitização é executada em segundo plano. Pode iniciar, parar e apresentar o estado do processo de sanitização. O processo de sanitização contém duas fases: A "fase de formatação" e a "fase de substituição do padrão".

Fase de formatação

A operação realizada para a fase de formatação depende da classe de disco sendo higienizado, como mostrado na tabela a seguir:

Classe de disco	Operação de fase de formatação
HDDs de capacidade	Ignorado
HDDs de performance	Operação de formato SCSI
SSDs	Operação de limpeza SCSI

Fase de substituição do padrão

Os padrões de substituição especificados são repetidos para o número especificado de ciclos.

Quando o processo de sanitização estiver concluído, os discos especificados estão em um estado higienizado. Eles não são devolvidos ao status de reposição automaticamente. Você deve devolver os discos

higienizados ao pool de reserva antes que os discos recém-higienizados estejam disponíveis para serem adicionados a outro agregado.

Quando a sanitização de disco não pode ser executada

A sanitização de disco não é suportada para todos os tipos de disco. Além disso, existem circunstâncias em que a sanitização de disco não pode ser realizada.

- Não é suportado em todos os números de peça SSD.

  Para obter informações sobre quais números de peça SSD suportam sanitização de disco, consulte "Hardware Universe" .

- Não é compatível com o modo de aquisição para sistemas de um par de HA.
- Ele não pode ser executado em discos que foram falhados devido a problemas de legibilidade ou de escrita.
- Ele não executa sua fase de formatação em unidades ATA.
- Se você estiver usando o padrão aleatório, ele não pode ser executado em mais de 100 discos de uma vez.
- Ele não é compatível com LUNs de array.
- Se você sanitizar ambos os discos SES na mesma prateleira ESH ao mesmo tempo, verá erros no console sobre o acesso a essa prateleira e avisos de prateleira não serão relatados durante o período de sanitização.

  No entanto, o acesso aos dados a esse compartimento não é interrompido.

O que acontece se a sanitização de disco for interrompida

Se a sanitização de disco for interrompida pela intervenção do usuário ou por um evento inesperado, como uma interrupção de energia, o ONTAP toma medidas para retornar os discos que estavam sendo higienizados para um estado conhecido, mas você também deve tomar medidas antes que o processo de sanitização possa terminar.

A sanitização de disco é uma operação de longa duração. Se o processo de sanitização for interrompido por falha de energia, pânico do sistema ou intervenção manual, o processo de sanitização deve ser repetido desde o início. O disco não é designado como higienizado.

Se a fase de formatação da sanitização de disco for interrompida, o ONTAP deverá recuperar todos os discos que foram corrompidos pela interrupção. Após a reinicialização do sistema e uma vez a cada hora, o ONTAP verifica se há algum disco alvo de sanitização que não concluiu a fase de formatação de sua sanitização. Se algum desses discos for encontrado, o ONTAP os recupera. O método de recuperação depende do tipo de disco. Depois que um disco é recuperado, você pode executar novamente o processo de sanitização nesse disco; para HDDs, você pode usar a `-s` opção para especificar que a fase de formatação não é repetida novamente.

Dicas para criar e fazer backup de camadas locais (agregados) contendo dados a serem higienizados

Se você estiver criando ou fazendo backup de camadas locais (agregados) para conter dados que possam precisar ser higienizados, seguir algumas diretrizes simples reduzirá o tempo necessário para higienizar seus dados.

- Certifique-se de que os níveis locais que contêm dados confidenciais não sejam maiores do que o necessário.

  Se forem maiores do que o necessário, a sanitização requer mais tempo, espaço em disco e largura de banda.

- Ao fazer backup de camadas locais que contêm dados confidenciais, evite fazer backup deles em níveis locais que também contenham grandes quantidades de dados não confidenciais.

  Isso reduz os recursos necessários para mover dados não confidenciais antes de higienizar dados confidenciais.

Sanitize um disco

A limpeza de um disco permite remover dados de um disco ou de um conjunto de discos em sistemas desativados ou inoperáveis para que os dados nunca possam ser recuperados.

Dois métodos estão disponíveis para higienizar discos usando a CLI:

Sanitize um disco com os comandos do modo de manutenção& n.o 8220; (versões ONTAP 9.8221 e posteriores)

Começando com ONTAP 9.6, você pode executar a sanitização de disco no modo de manutenção.

Antes de começar

- Os discos não podem ser discos com autocriptografia (SED).

  Você deve usar o `storage encryption disk sanitize` comando para higienizar um SED.

  "Criptografia de dados em repouso"

Passos

1. Arranque no modo de manutenção.
   a. Saia do shell atual entrando `halt`em .

      O prompt Loader é exibido.

   b. Entre no modo de manutenção entrando `boot_ontap maint`em .

      Depois de algumas informações serem exibidas, o prompt do modo de manutenção é exibido.

2. Se os discos que você deseja limpar estiverem particionados, desparticione cada disco:

   > O comando para desparticionar um disco só está disponível no nível de diag e só deve ser executado sob supervisão de suporte NetApp. É altamente recomendável que você entre em Contato com o suporte da NetApp antes de prosseguir. Você também pode consultar o artigo da base de dados de Conhecimento "Como desparticionar uma unidade sobressalente no ONTAP"

   ```
   disk unpartition <disk_name>
   ```

3. Higienizar os discos especificados:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

   > Não desligue a alimentação do nó, interrompa a conectividade do storage ou remova os discos de destino durante a limpeza. Se a limpeza for interrompida durante a fase de formatação, a fase de formatação deve ser reiniciada e pode ser concluída antes que os discos sejam higienizados e prontos para serem devolvidos ao pool sobressalente. Se você precisar abortar o processo de sanitização, você pode fazê-lo usando o `disk sanitize abort` comando. Se os discos especificados estiverem passando pela fase de formatação da sanitização, o cancelamento não ocorrerá até que a fase esteja concluída.

`-p` `<pattern1>` `-p` `<pattern2>` `-p` `<pattern3>` especifica um ciclo de um a três padrões de substituição de bytes hexadecimais definidos pelo usuário que podem ser aplicados sucessivamente aos discos que estão sendo higienizados. O padrão padrão padrão é três passagens, usando 0x55 para a primeira passagem, 0xaa para a segunda passagem e 0x3c para a terceira passagem.

`-r` substitui uma substituição padronizada por uma substituição aleatória para qualquer ou todos os passes.

`-c <cycle_count>` especifica o número de vezes que os padrões de substituição especificados são aplicados. O valor padrão é um ciclo. O valor máximo é de sete ciclos.

`<disk_list>` Especifica uma lista separada por espaço das IDs dos discos sobressalentes a serem higienizados.

4. Se desejar, verifique o estado do processo de sanitização de disco:

   ```
   disk sanitize status [<disk_list>]
   ```

5. Depois que o processo de sanitização estiver concluído, retorne os discos ao status de reserva para cada disco:

   ```
   disk sanitize release <disk_name>
   ```

6. Sair do modo de manutenção.

Higienize um disco com os comandos e n.o 8220;nodeshell& n.o 8221; (todas as versões do ONTAP 9)

Depois que o recurso de sanitização de disco é ativado usando comandos nodeshell em um nó, ele não pode ser desativado.

Antes de começar

- Os discos devem ser discos sobressalentes; eles devem ser de propriedade de um nó, mas não usados em um nível local (agregado).

  Se os discos forem particionados, nenhuma partição poderá ser usada em um nível local (agregado).

- Os discos não podem ser discos com autocriptografia (SED).

  Você deve usar o `storage encryption disk sanitize` comando para higienizar um SED.

  "Criptografia de dados em repouso"

- Os discos não podem fazer parte de um pool de armazenamento.

Passos

1. Se os discos que você deseja limpar estiverem particionados, desparticione cada disco:

   > O comando para desparticionar um disco só está disponível no nível de diag e só deve ser executado sob supervisão de suporte NetApp. **É altamente recomendável que você entre em Contato com o suporte da NetApp antes de prosseguir.** Você também pode consultar o artigo da base de dados de Conhecimento "Como desparticionar uma unidade sobressalente no ONTAP".

   ```
   disk unpartition <disk_name>
   ```

2. Introduza o nodeshell para o nó que possui os discos que pretende higienizar:

   ```
   system node run -node <node_name>
   ```

3. Ativar sanitização de disco:

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   Você é solicitado a confirmar o comando porque ele é irreversível.

4. Mude para o nível de privilégio avançado nodeshell:

   ```
   priv set advanced
   ```

5. Higienizar os discos especificados:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

Não desligue a alimentação do nó, interrompa a conectividade do storage ou remova os discos de destino durante a limpeza. Se a limpeza for interrompida durante a fase de formatação, a fase de formatação deve ser reiniciada e pode ser concluída antes que os discos sejam higienizados e prontos para serem devolvidos ao pool sobressalente. Se você precisar abortar o processo de sanitização, você pode fazê-lo usando o comando Disk Sanitize abort. Se os discos especificados estiverem passando pela fase de formatação da sanitização, o cancelamento não ocorrerá até que a fase esteja concluída.

`-p <pattern1> -p <pattern2> -p <pattern3>` especifica um ciclo de um a três padrões de substituição de bytes hexadecimais definidos pelo usuário que podem ser aplicados sucessivamente aos discos que estão sendo higienizados. O padrão padrão padrão é três passagens, usando 0x55 para a primeira passagem, 0xaa para a segunda passagem e 0x3c para a terceira passagem.

`-r` substitui uma substituição padronizada por uma substituição aleatória para qualquer ou todos os passes.

`-c <cycle_count>` especifica o número de vezes que os padrões de substituição especificados são aplicados.

O valor padrão é um ciclo. O valor máximo é de sete ciclos.

`<disk_list>` Especifica uma lista separada por espaço das IDs dos discos sobressalentes a serem higienizados.

6. Se pretender verificar o estado do processo de sanitização de disco:

   ```
   disk sanitize status [<disk_list>]
   ```

7. Depois de concluir o processo de sanitização, devolva os discos ao estado de reserva:

   ```
   disk sanitize release <disk_name>
   ```

8. Retornar ao nível de privilégio de administrador nodeshell:

   ```
   priv set admin
   ```

9. Voltar à CLI do ONTAP:

   ```
   exit
   ```

10. Determine se todos os discos foram retornados ao status de reserva:

    ```
    storage aggregate show-spare-disks
    ```

Se…	Então…
Todos os discos higienizados são listados como peças sobressalentes	Você está pronto. Os discos são higienizados e em estado sobressalente.

Alguns dos discos higienizados não são listados como sobressalentes	Execute as seguintes etapas:
	a. Entrar no modo de privilégio avançado:
	`set -privilege advanced`
	b. Atribua os discos higienizados não atribuídos ao nó apropriado para cada disco:
	`storage disk assign -disk <disk_name> -owner <node_name>`
	c. Retorne os discos ao status de reserva para cada disco:
	`storage disk unfail -disk <disk_name> -s -q`
	d. Voltar ao modo administrativo:
	`set -privilege admin`

Resultado

Os discos especificados são higienizados e designados como hot spares. Os números de série dos discos higienizados são gravados em `/etc/log/sanitized_disks`.

Os logs de sanitização dos discos especificados, que mostram o que foi concluído em cada disco, são gravados no `/mroot/etc/log/sanitization.log`.

Comandos para gerenciar discos

Você pode usar os `storage disk` comandos e `storage aggregate` para gerenciar seus discos.

Se você quiser…	Use este comando…
Exibir uma lista de discos sobressalentes, incluindo discos particionados, pelo proprietário	`storage aggregate show-spare-disks`
Exibir o tipo de RAID do disco, o uso atual e o grupo RAID por agregado	`storage aggregate show-status`
Exibir o tipo de RAID, uso atual, agregado e grupo RAID, incluindo peças sobressalentes, para discos físicos	`storage disk show -raid`
Exibir uma lista de discos com falha	`storage disk show -broken`

Apresentar o nome da unidade do pré-cluster (nodescope) para um disco	`storage disk show -primary-paths` (avançado)
Acenda o LED de um determinado disco ou prateleira	`storage disk set-led`
Exiba o tipo de checksum de um disco específico	`storage disk show -fields checksum-compatibility`
Exiba o tipo de checksum para todos os discos sobressalentes	`storage disk show -fields checksum-compatibility -container-type spare`
Exibir informações de conetividade e posicionamento do disco	`storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay`
Exibir os nomes de discos do pré-cluster para discos específicos	`storage disk show -disk diskname -fields diskpathnames`
Apresentar a lista de discos no centro de manutenção	`storage disk show -maintenance`
Exibir a vida útil do SSD	`storage disk show -ssd-wear`
Desparticionar um disco compartilhado	`storage disk unpartition` (disponível no nível de diagnóstico)
Zero todos os discos não zerados	`storage disk zerospares`
Parar um processo de sanitização contínuo em um ou mais discos especificados	`system node run -node nodename -command disk sanitize`
Exibir informações do disco de criptografia de armazenamento	`storage encryption disk show`
Recuperar chaves de autenticação de todos os servidores de gerenciamento de chaves vinculados	`security key-manager restore`

Informações relacionadas

- "Referência do comando ONTAP"

Comandos para exibir informações de uso de espaço

Você usa `storage aggregate` os comandos e `volume` para ver como o espaço está sendo usado em agregados, volumes e cópias Snapshot delas.

Para exibir informações sobre…	Use este comando…

Agregados, incluindo detalhes sobre porcentagens de espaço usado e disponível, tamanho da reserva do Snapshot e outras informações de utilização de espaço	`storage aggregate show` `storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`
Como discos e grupos RAID são usados em um agregado e status RAID	`storage aggregate show-status`
A quantidade de espaço em disco que seria recuperada se você excluísse uma cópia Snapshot específica	`volume snapshot compute-reclaimable`
A quantidade de espaço utilizada por um volume	`volume show -fields size,used,available,percent-used` `volume show-space`
A quantidade de espaço usada por um volume no agregado que contém	`volume show-footprint`

Informações relacionadas

- "Referência do comando ONTAP"

Comandos para exibir informações sobre prateleiras de armazenamento

Use o `storage shelf show` comando para exibir informações de configuração e erro para as gavetas de disco.

Se você quiser exibir…	Use este comando…
Informações gerais sobre a configuração do compartimento e o status do hardware	`storage shelf show`
Informações detalhadas para um compartimento específico, incluindo ID da pilha	`storage shelf show -shelf`
Erros não resolvidos, acionáveis pelo cliente, por compartimento	`storage shelf show -errors`
Informações sobre a baía	`storage shelf show -bay`
Informações de conetividade	`storage shelf show -connectivity`
Informações de refrigeração, incluindo sensores de temperatura e ventoinhas de arrefecimento	`storage shelf show -cooling`
Informações sobre módulos de e/S.	`storage shelf show -module`

Se você quiser exibir…	Use este comando…
Informações da porta	`storage shelf show -port`
Informações de energia, incluindo PSUs (unidades de fonte de alimentação), sensores de corrente e sensores de tensão	`storage shelf show -power`

Informações relacionadas

- "Referência do comando ONTAP"

Gerenciar configurações RAID

Visão geral do gerenciamento de configurações RAID

Você pode executar vários procedimentos para gerenciar configurações RAID em seu sistema.

- **Aspectos do gerenciamento de configurações RAID**:
  - "Políticas RAID padrão para camadas locais (agregados)"
  - "Níveis de proteção RAID para discos"
- **Informações de unidade e grupo RAID para um nível local (agregado)**
  - "Determinar informações de unidade e grupo RAID para um nível local (agregado)"
- **Conversões de configuração RAID**
  - "Converter de RAID-DP em RAID-teC"
  - "Converter de RAID-teC em RAID-DP"
- **Dimensionamento do grupo RAID**
  - "Considerações para dimensionar grupos RAID"
  - "Personalize o tamanho do seu grupo RAID"

Políticas RAID padrão para camadas locais (agregados)

RAID-DP ou RAID-teC é a política RAID padrão para todas as novas camadas locais (agregados). A política RAID determina a proteção de paridade que você tem em caso de falha de disco.

O RAID-DP fornece proteção de paridade dupla no caso de uma falha de disco única ou dupla. RAID-DP é a política RAID padrão para os seguintes tipos de camada local (agregado):

- Categorias locais all-flash
- Camadas locais do Flash Pool
- Camadas locais da unidade de disco rígido (HDD) de desempenho

O RAID-teC é compatível com todos os tipos de disco e todas as plataformas, incluindo AFF. Camadas locais que contêm discos maiores têm maior possibilidade de falhas simultâneas de disco. O RAID-teC ajuda a mitigar esse risco, fornecendo proteção de paridade tripla para que seus dados possam sobreviver a até três

falhas simultâneas de disco. RAID-teC é a política RAID padrão para camadas locais de HDD de capacidade com discos de 6 TB ou maiores.

Cada tipo de política RAID requer um número mínimo de discos:

- RAID-DP: Mínimo de 5 discos
- RAID-teC: Mínimo de 7 discos

Níveis de proteção RAID para discos

O ONTAP é compatível com três níveis de proteção RAID para camadas locais (agregados). O nível de proteção RAID determina o número de discos de paridade disponíveis para recuperação de dados em caso de falhas de disco.

Com a proteção RAID, se houver uma falha de disco de dados em um grupo RAID, o ONTAP poderá substituir o disco com falha por um disco sobressalente e usar dados de paridade para reconstruir os dados do disco com falha.

- **RAID4**

  Com a proteção RAID4, o ONTAP pode usar um disco sobressalente para substituir e reconstruir os dados de um disco com falha no grupo RAID.

- **RAID-DP**

  Com a proteção RAID-DP, o ONTAP pode usar até dois discos sobressalentes para substituir e reconstruir os dados de até dois discos com falha simultânea no grupo RAID.

- **RAID-TEC**

  Com a proteção RAID-teC, o ONTAP pode usar até três discos sobressalentes para substituir e reconstruir os dados de até três discos com falha simultânea no grupo RAID.

Informações de unidade e grupo RAID para um nível local (agregado)

Algumas tarefas de administração de camadas locais (agregadas) exigem que você saiba quais tipos de unidades compõem o nível local, seu tamanho, checksum e status, se eles são compartilhados com outros níveis locais e o tamanho e a composição dos grupos RAID.

Passo

1. Mostrar as unidades para o agregado, por grupo RAID:

   `storage aggregate show-status` *`aggr_name`*

   As unidades são exibidas para cada grupo RAID no agregado.

   Você pode ver o tipo RAID da unidade (dados, paridade, dparidade) `Position` na coluna. Se a `Position` coluna for exibida `shared`, a unidade será compartilhada: Se for um disco rígido, será um disco particionado; se for um SSD, ele fará parte de um pool de armazenamento.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                 Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11      0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                 Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13      0   SSD        -  186.2GB  745.2GB (normal)
     shared   2.0.12      0   SSD        -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

Converter de RAID-DP em RAID-teC

Se você quiser obter proteção adicional de paridade tripla, poderá converter de RAID-DP em RAID-teC. O RAID-teC é recomendado se o tamanho dos discos usados em seu nível local (agregado) for maior que 4 TIB.

O que você vai precisar

O nível local (agregado) que deve ser convertido deve ter no mínimo sete discos.

Sobre esta tarefa

- As camadas locais da unidade de disco rígido (HDD) podem ser convertidas de RAID-DP para RAID-teC. Isso inclui camadas de HDD nos níveis locais do Flash Pool.
- Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/storage-Aggregate-modify.html[`storage aggregate modify` na referência de comando ONTAP.

Passos

1. Verifique se o agregado está on-line e tem no mínimo seis discos:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Converta o agregado de RAID-DP em RAID-teC:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

3. Verifique se a política de RAID agregado é RAID-teC:

```
storage aggregate show aggregate_name
```

Converter de RAID-teC em RAID-DP

Se você reduzir o tamanho do seu nível local (agregado) e não precisar mais de tripla paridade, poderá converter sua política de RAID-teC em RAID-DP e reduzir o número de discos necessários para paridade RAID.

O que você vai precisar

O tamanho máximo do grupo RAID para RAID-teC é maior do que o tamanho máximo do grupo RAID para RAID-DP. Se o maior tamanho de grupo RAID-teC não estiver dentro dos limites RAID-DP, você não poderá converter para RAID-DP.

Sobre esta tarefa

Para entender as implicações da conversão entre tipos de RAID, consulte o "parâmetros" para obter o `storage aggregate modify` comando.

Passos

1. Verifique se o agregado está on-line e tem no mínimo seis discos:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Converter o agregado de RAID-teC em RAID-DP:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

3. Verifique se a política RAID agregada é RAID-DP:

```
storage aggregate show aggregate_name
```

Considerações para dimensionar grupos RAID

A configuração de um tamanho de grupo RAID ideal requer uma troca de fatores. Você precisa decidir quais fatores - velocidade da reconstrução RAID, garantia contra risco de perda de dados devido a falha da unidade, otimização do desempenho de e/S e maximização do espaço de storage de dados - são mais importantes para o agregado (camada local) que você está configurando.

Ao criar grupos RAID maiores, você maximiza o espaço disponível para armazenamento de dados para a mesma quantidade de armazenamento usada para paridade (também conhecido como o "'imposto de paridade"). Por outro lado, quando um disco falha em um grupo RAID maior, o tempo de reconstrução é aumentado, afetando o desempenho por um período de tempo maior. Além disso, ter mais discos em um grupo RAID aumenta a probabilidade de uma falha de vários discos dentro do mesmo grupo RAID.

Grupos RAID de HDD ou LUN de matriz

Siga estas diretrizes ao dimensionar seus grupos RAID compostos por HDDs ou LUNs de storage:

- Todos os grupos RAID em um nível local (agregado) devem ter o mesmo número de discos.

  Embora você possa ter até 50% menos ou mais do que o número de discos em diferentes grupos raid em um nível local, isso pode levar a gargalos de desempenho em alguns casos, por isso é melhor evitado.

- O intervalo recomendado de números de discos do grupo RAID está entre 12 e 20.

  A confiabilidade dos discos de desempenho pode suportar um tamanho de grupo RAID de até 28 TB, se necessário.

- Se você puder satisfazer as duas primeiras diretrizes com vários números de disco do grupo RAID, escolha o número maior de discos.

Grupos RAID de SSD em camadas locais (agregados) do Flash Pool

O tamanho do grupo RAID SSD pode ser diferente do tamanho do grupo RAID para os grupos RAID de HDD em um nível local do Flash Pool (agregado). Normalmente, você deve garantir que tenha apenas um grupo RAID SSD para uma camada local de Flash Pool, para minimizar o número de SSDs necessários para a paridade.

Grupos RAID SSD em camadas locais de SSD (agregados)

Você deve seguir estas diretrizes ao dimensionar seus grupos RAID compostos de SSDs:

- Todos os grupos RAID em um nível local (agregado) devem ter um número semelhante de unidades.

  Os grupos RAID não precisam ter exatamente o mesmo tamanho, mas você deve evitar ter qualquer grupo RAID que tenha menos de metade do tamanho de outros grupos RAID no mesmo nível local, quando possível.

- Para RAID-DP, o intervalo recomendado de tamanho do grupo RAID é entre 20 e 28.

Personalize o tamanho dos grupos RAID

Você pode personalizar o tamanho dos grupos RAID para garantir que os tamanhos dos grupos RAID sejam apropriados para a quantidade de storage que você planeja incluir em um nível local (agregado).

Sobre esta tarefa

Para camadas locais padrão (agregados), você altera o tamanho dos grupos RAID para cada categoria local separadamente. Para camadas locais do Flash Pool, é possível alterar o tamanho do grupo RAID para os grupos RAID SSD e RAID HDD de forma independente.

A lista a seguir descreve alguns fatos sobre como alterar o tamanho do grupo RAID:

- Por padrão, se o número de discos ou LUNs de matriz no grupo RAID criado mais recentemente for menor do que o novo tamanho do grupo RAID, os discos ou LUNs de matriz serão adicionados ao grupo RAID criado mais recentemente até atingir o novo tamanho.
- Todos os outros grupos RAID existentes nesse nível local permanecem do mesmo tamanho, a menos que você explicitamente adicione discos a eles.

- Nunca é possível fazer com que um grupo RAID fique maior do que o tamanho máximo atual do grupo RAID para o nível local.
- Não é possível diminuir o tamanho dos grupos RAID já criados.
- O novo tamanho se aplica a todos os grupos RAID nesse nível local (ou, no caso de um nível local do Flash Pool, todos os grupos RAID para o tipo de grupo RAID afetado - SSD ou HDD).

Passos

1. Use o comando aplicável:

Se você quiser…	Digite o seguinte comando…
Altere o tamanho máximo do grupo RAID para os grupos RAID SSD de um agregado Flash Pool	`storage aggregate modify -aggregate aggr_name -cache-raid-group-size size`
Altere o tamanho máximo de quaisquer outros grupos RAID	`storage aggregate modify -aggregate aggr_name -maxraidsize size`

Exemplos

O comando a seguir altera o tamanho máximo do grupo RAID do agregado n1_A4 para 20 discos ou LUNs de matriz:

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

O comando a seguir altera o tamanho máximo do grupo RAID dos grupos RAID de cache SSD do Flash Pool Aggregate n1_cache_A2 para 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

Gerenciar camadas locais (agregados) do Flash Pool

Gerenciar camadas de Flash Pool (agregados)

É possível executar vários procedimentos para gerenciar camadas de Flash Pool (agregados) no sistema.

- **Políticas de armazenamento em cache**
  - "Políticas de armazenamento em cache de camada local (agregado) do Flash Pool"
  - "Gerenciar políticas de armazenamento em cache do Flash Pool"
- * Partição SSD*
  - "Particionamento de SSD do Flash Pool para camadas locais (agregados) do Flash Pool usando pools de storage"
- * Candidatura e tamanho do cache*
  - "Determine a candidatura do Flash Pool e o tamanho ideal do cache"
- * Criação de Flash Pool*
  - "Criar um nível local (agregado) do Flash Pool usando SSDs físicos"
  - "Criar uma camada local (agregado) do Flash Pool usando pools de storage de SSD"

Políticas de armazenamento em cache de camada local (agregado) do Flash Pool

As políticas de armazenamento em cache para os volumes em uma camada local do Flash Pool (agregado) permitem que você implante o Flash como um cache de alta performance para seu conjunto de dados em trabalho, ao mesmo tempo em que usa HDDs de baixo custo para dados acessados com menos frequência. Se você estiver fornecendo cache para duas ou mais camadas locais do Flash Pool, use o particionamento SSD do Flash Pool para compartilhar SSDs entre as camadas locais no Flash Pool.

As políticas de armazenamento em cache são aplicadas a volumes que residem nas camadas locais do Flash Pool. Você deve entender como as políticas de armazenamento em cache funcionam antes de alterá-las.

Na maioria dos casos, a política de cache padrão de "'auto'" é a melhor política de armazenamento em cache a ser usada. A política de armazenamento em cache só deve ser alterada se uma política diferente fornecer melhor performance para seu workload. A configuração da política de armazenamento em cache errada pode degradar gravemente o desempenho do volume; a degradação do desempenho pode aumentar gradualmente ao longo do tempo.

As políticas de armazenamento em cache combinam uma política de armazenamento em cache de leitura e uma política de armazenamento em cache de gravação. O nome da política concatena os nomes da política de armazenamento em cache de leitura e da política de armazenamento em cache de escrita, separados por um hífen. Se não houver nenhum hífen no nome da política, a política de cache de gravação é "nenhum", exceto para a política "auto".

As políticas de armazenamento em cache para leitura otimizam para a performance de leitura futura, colocando uma cópia dos dados no cache, além dos dados armazenados em HDDs. Para políticas de cache de leitura que inserem dados no cache para operações de gravação, o cache opera como um cache *write-through*.

Os dados inseridos no cache usando a política de armazenamento em cache de gravação só existem no cache; não há cópia em HDDs. O cache do Flash Pool está protegido por RAID. A ativação do armazenamento em cache de gravação torna os dados das operações de gravação disponíveis para leituras do cache imediatamente, ao mesmo tempo em que atrasa a gravação dos dados em HDDs até que eles fiquem fora do cache.

Se você mover um volume de um nível local do Flash Pool para um nível local de nível único, ele perderá sua política de armazenamento em cache; se você mais tarde movê-lo de volta para um nível local do Flash Pool, será atribuída a política de armazenamento em cache padrão de "'auto". Se você mover um volume entre dois níveis local do Flash Pool, a política de armazenamento em cache será preservada.

Alterar uma política de armazenamento em cache

Você pode usar a CLI para alterar a política de armazenamento em cache de um volume que reside em um nível local do Flash Pool usando o `-caching-policy` parâmetro com o `volume create` comando.

Quando você cria um volume em um nível local do Flash Pool, por padrão, a política de armazenamento em cache ""automático"" é atribuída ao volume.

Gerenciar políticas de armazenamento em cache do Flash Pool

Visão geral do gerenciamento de políticas de armazenamento em cache do Flash Pool

Com a CLI, você pode executar vários procedimentos para gerenciar as políticas de armazenamento em cache do Flash Pool no sistema.

- **Preparação**
  - "Determinar se deseja modificar a política de armazenamento em cache das camadas locais (agregados) do Flash Pool"
- **Alteração das políticas de cache**
  - "Modificar políticas de armazenamento em cache de camadas locais (agregados) do Flash Pool"
  - "Definir a política de retenção de cache para camadas locais (agregados) do Flash Pool"

Determinar se deseja modificar a política de armazenamento em cache das camadas locais (agregados) do Flash Pool

Você pode atribuir políticas de retenção de cache a volumes nas camadas locais (agregados) do Flash Pool para determinar por quanto tempo os dados de volume permanecem no cache do Flash Pool. No entanto, em alguns casos, alterar a política de retenção de cache pode não afetar o tempo que os dados do volume permanecem no cache.

Sobre esta tarefa

Se seus dados atenderem a qualquer uma das seguintes condições, alterar sua política de retenção de cache pode não ter impactos:

- Sua carga de trabalho é sequencial.
- Sua carga de trabalho não releia os blocos aleatórios armazenados em cache nas unidades de estado sólido (SSDs).
- O tamanho do cache do volume é muito pequeno.

Passos

As etapas a seguir verificam as condições que devem ser atendidas pelos dados. A tarefa deve ser feita usando a CLI no modo de privilégio avançado.

1. Use a CLI para exibir o volume de carga de trabalho:

   ```
   statistics start -object workload_volume
   ```

2. Determine o padrão de carga de trabalho do volume:

   ```
   statistics show -object workload_volume -instance volume-workload -counter
   sequential_reads
   ```

3. Determine a taxa de acerto do volume:

   ```
   statistics show -object wafl_hya_vvol -instance volume -counter
   read_ops_replaced_pwercent|wc_write_blks_overwritten_percent
   ```

4. Determine o `Cacheable Read` e `Project Cache Alloc` do volume:

   ```
   system node run -node node_name wafl awa start aggr_name
   ```

5. Apresentar o resumo AWA:

   `system node run -node node_name wafl awa print aggr_name`

6. Compare a taxa de acerto do volume com a `Cacheable Read`.

   Se a taxa de acertos do volume for maior que o `Cacheable Read`, a carga de trabalho não releia os blocos aleatórios armazenados em cache nos SSDs.

7. Compare o tamanho atual do cache do volume com o `Project Cache Alloc`.

   Se o tamanho atual do cache do volume for maior do que o `Project Cache Alloc`, o tamanho do cache de volume será muito pequeno.

Modificar políticas de armazenamento em cache de camadas locais (agregados) do Flash Pool

Você deve modificar a política de armazenamento em cache de um volume somente se uma política de armazenamento em cache diferente for esperada para fornecer melhor desempenho. Você pode modificar a política de armazenamento em cache de um volume em um nível local do Flash Pool (agregado).

O que você vai precisar

Você deve determinar se deseja modificar sua política de armazenamento em cache.

Sobre esta tarefa

Na maioria dos casos, a política de cache padrão de "'auto'" é a melhor política de cache que você pode usar. A política de armazenamento em cache só deve ser alterada se uma política diferente fornecer melhor performance para seu workload. A configuração da política de armazenamento em cache errada pode degradar gravemente o desempenho do volume; a degradação do desempenho pode aumentar gradualmente ao longo do tempo. Você deve ter cuidado ao modificar políticas de armazenamento em cache. Se você tiver problemas de desempenho com um volume para o qual a política de armazenamento em cache foi alterada, você deverá retornar a política de armazenamento em cache para "'auto'".

Passo

1. Use a CLI para modificar a política de armazenamento em cache do volume:

   `volume modify -volume volume_name -caching-policy policy_name`

Exemplo

O exemplo a seguir modifica a política de armazenamento em cache de um volume chamado "'vol2'" para a política "'none'":

```
volume modify -volume vol2 -caching-policy none
```

Definir a política de retenção de cache para camadas locais (agregados) do Flash Pool

Você pode atribuir políticas de retenção de cache a volumes nas camadas locais (agregados) do Flash Pool. Os dados em volumes com uma política de alta retenção de cache permanecem no cache por mais tempo e os dados em volumes com uma política de baixa retenção de cache são removidos mais cedo. Isso aumenta o desempenho de

seus workloads críticos, pois as informações de alta prioridade são acessíveis a uma taxa mais rápida por um período mais longo.

O que você vai precisar

Você deve saber se o seu sistema tem quaisquer condições que possam impedir que a política de retenção de cache tenha um impactos sobre quanto tempo seus dados permanecem no cache.

Passos

Use a CLI no modo de privilégio avançado para executar as seguintes etapas:

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Verifique a política de retenção de cache do volume:

   Por padrão, a política de retenção de cache é "normal".

3. Defina a política de retenção de cache:

Versão de ONTAP	Comando
ONTAP 9.0, 9,1	`priority hybrid-cache set volume_name read-cache=read_cache_value write-cache=write_cache_value cache-retention-priority=cache_retention_policy` Defina `cache_retention_policy` como `high` para os dados que você deseja permanecer no cache por mais tempo. Defina `cache_retention_policy` como `low` para os dados que você deseja remover do cache mais cedo.
ONTAP 9 .2 ou posterior	`volume modify -volume volume_name -vserver vserver_name -caching-policy policy_name.`

4. Verifique se a política de retenção de cache do volume foi alterada para a opção selecionada.
5. Retornar a configuração de privilégio para admin:

   ```
   set -privilege admin
   ```

Particionamento de SSD do Flash Pool para camadas locais (agregados) do Flash Pool usando pools de storage

Se você estiver fornecendo cache para duas ou mais camadas locais de Flash Pool (agregados), use o particionamento de unidade de estado sólido (SSD) do Flash Pool. O particionamento de SSD do Flash Pool permite que os SSDs sejam compartilhados por

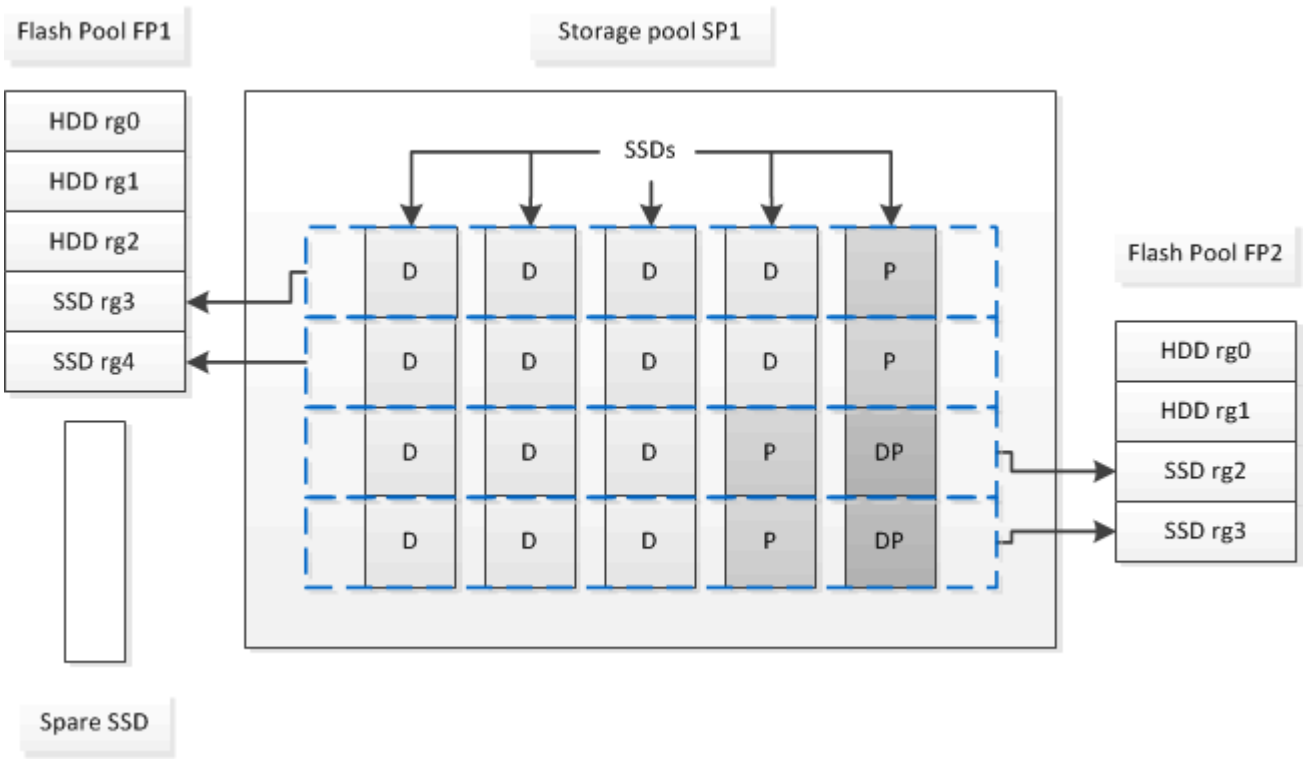
todos os níveis locais que usam o Flash Pool. Isso espalha o custo da paridade em vários níveis locais, aumenta a flexibilidade de alocação de cache SSD e maximiza o desempenho do SSD.

Para que um SSD seja usado em um nível local de Flash Pool, o SSD deve ser colocado em um pool de storage. Você não pode usar SSDs que foram particionados para particionamento de dados raiz em um pool de armazenamento. Depois que o SSD é colocado no pool de armazenamento, o SSD não pode mais ser gerenciado como um disco autônomo e não pode ser removido do pool de armazenamento, a menos que você destrua os níveis locais associados ao Flash Pool e destrua o pool de armazenamento.

Os pools de armazenamento SSD são divididos em quatro unidades de alocação iguais. Os SSDs adicionados ao pool de armazenamento são divididos em quatro partições e uma partição é atribuída a cada uma das quatro unidades de alocação. Os SSDs no pool de storage precisam pertencer ao mesmo par de HA. Por padrão, duas unidades de alocação são atribuídas a cada nó no par de HA. As unidades de alocação devem ser de propriedade do nó que possui o nível local que está atendendo. Se mais cache Flash for necessário para camadas locais em um dos nós, o número padrão de unidades de alocação pode ser deslocado para diminuir o número em um nó e aumentar o número no nó do parceiro.

Você usa SSDs sobressalentes para adicionar a um pool de armazenamento SSD. Se o pool de storage fornecer unidades de alocação para as camadas locais do Flash Pool de propriedade de ambos os nós do par de HA, os SSDs sobressalentes poderão pertencer a qualquer um dos nós. No entanto, se o pool de storage fornecer unidades de alocação apenas para as camadas locais do Flash Pool de propriedade de um dos nós do par de HA, os componentes sobressalentes SSD precisarão pertencer ao mesmo nó.

A ilustração a seguir é um exemplo de particionamento do Flash Pool SSD. O pool de armazenamento SSD fornece cache para dois níveis locais do Flash Pool:



O pool de armazenamento SP1 é composto por cinco SSDs e um SSD hot spare. Duas das unidades de alocação do pool de storage são alocadas ao Flash Pool FP1 e duas são alocadas ao Flash Pool FP2. FP1 tem um tipo de cache RAID de RAID4. Portanto, as unidades de alocação fornecidas a FP1 contêm apenas uma partição designada para paridade. O FP2 tem um tipo RAID de cache de RAID-DP. Portanto, as unidades

de alocação fornecidas ao FP2 incluem uma partição de paridade e uma partição de paridade dupla.

Neste exemplo, duas unidades de alocação são alocadas a cada nível local do Flash Pool. No entanto, se um nível local do Flash Pool exigir um cache maior, você poderá alocar três das unidades de alocação a esse nível local do Flash Pool e apenas uma para o outro.

Determine a candidatura do Flash Pool e o tamanho ideal do cache

Antes de converter um nível local (agregado) existente em um nível local do Flash Pool, você pode determinar se o nível local está vinculado a e/S e o melhor tamanho de cache do Flash Pool para seu workload e orçamento. Você também pode verificar se o cache de um nível local do Flash Pool existente é dimensionado corretamente.

O que você vai precisar

Você deve saber aproximadamente quando o nível local que você está analisando experimenta sua carga máxima.

Passos

1. Entrar no modo avançado:

   ```
   set advanced
   ```

2. Se você precisar determinar se um nível local (agregado) existente seria um bom candidato para conversão em um agregado de Flash Pool, determine o quão ocupados os discos no agregado estão durante um período de pico de carga e como isso está afetando a latência:

   ```
   statistics show-periodic -object disk:raid_group -instance raid_group_name
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

   Você pode decidir se reduzir a latência adicionando o cache Flash Pool faz sentido para esse agregado.

   O comando a seguir mostra as estatísticas do primeiro grupo RAID do agregado "'aggr1":

   ```
   statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

3. Inicie o Automated Workload Analyzer (AWA):

   ```
   storage automated-working-set-analyzer start -node node_name -aggregate
   aggr_name
   ```

   A AWA começa a coletar dados da carga de trabalho para os volumes associados ao agregado especificado.

4. Sair do modo avançado:

   ```
   set admin
   ```

   Permita que o AWA funcione até que um ou mais intervalos de pico de carga tenham ocorrido. O AWA coleta estatísticas de carga de trabalho para os volumes associados ao agregado especificado e analisa dados por até uma semana de duração. Executar AWA por mais de uma semana irá relatar apenas os dados coletados da semana mais recente. As estimativas de tamanho do cache baseiam-se nas cargas mais altas observadas durante o período de coleta de dados; a carga não precisa ser alta para todo o

período de coleta de dados.

5. Entrar no modo avançado:

   ```
   set advanced
   ```

6. Exibir a análise da carga de trabalho:

   ```
   storage automated-working-set-analyzer show -node node_name -instance
   ```

7. Parar AWA:

   ```
   storage automated-working-set-analyzer stop node_name
   ```

   Todos os dados de workload são limpos e não estão mais disponíveis para análise.

8. Sair do modo avançado:

   ```
   set admin
   ```

Criar um nível local (agregado) do Flash Pool usando SSDs físicos

Você cria um nível local do Flash Pool (agregado) habilitando o recurso em um nível local existente composto por grupos RAID de HDD e adicionando um ou mais grupos RAID de SSD a esse nível local. Isso resulta em dois conjuntos de grupos RAID para esse nível local: Grupos RAID SSD (cache SSD) e grupos RAID HDD.

Sobre esta tarefa

Depois de adicionar um cache SSD a um nível local para criar um nível local do Flash Pool, não é possível remover o cache SSD para converter o nível local de volta à configuração original.

Por padrão, o nível RAID do cache SSD é o mesmo que o nível RAID dos grupos RAID HDD. Você pode substituir essa seleção padrão especificando a opção "'raidtype'" quando você adiciona os primeiros grupos RAID SSD.

Antes de começar

- Você precisa ter identificado um nível local válido composto de HDDs para converter em um nível local de Flash Pool.
- Você precisa ter determinado a qualificação para o armazenamento em cache de gravação dos volumes associados ao nível local e concluído as etapas necessárias para resolver problemas de qualificação.
- Você precisa ter determinado os SSDs que você estará adicionando e esses SSDs devem pertencer ao nó no qual você está criando a camada local do Flash Pool.
- Você precisa ter determinado os tipos de checksum dos SSDs que está adicionando e dos HDDs que já estão no nível local.
- Você deve ter determinado o número de SSDs que está adicionando e o tamanho ideal do grupo RAID para os grupos RAID SSD.

  O uso de menos grupos RAID no cache SSD reduz o número de discos de paridade necessários, mas grupos RAID maiores exigem RAID-DP.

- Você deve ter determinado o nível RAID que deseja usar para o cache SSD.

- Você deve ter determinado o tamanho máximo de cache para o seu sistema e determinado que adicionar cache SSD ao seu nível local não fará com que você o exceda.
- Você precisa se familiarizar com os requisitos de configuração das camadas locais do Flash Pool.

Passos

Você pode criar um agregado do FlashPool usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

A partir do ONTAP 9.12,1, você pode usar o Gerenciador de sistema para criar um nível local de pool flash usando SSDs físicos.

Passos

1. Selecione **Storage > Tiers** e, em seguida, selecione um nível de armazenamento HDD local existente.
2. Selecione **Add Flash Pool Cache**.
3. Selecione **Use SSDs dedicados como cache**.
4. Selecione um tipo de disco e o número de discos.
5. Escolha um tipo RAID.
6. Selecione **Guardar**.
7. Localize a camada de storage e selecione .
8. Selecione **mais detalhes**. Verifique se o Flash Pool é exibido como **Enabled**.

CLI

Passos

1. Marque o nível local (agregado) como qualificado para se tornar um agregado de Flash Pool:

   `storage aggregate modify -aggregate` *`aggr_name`* `-hybrid-enabled true`

   Se essa etapa não for bem-sucedida, determine a qualificação para o armazenamento em cache de gravação para o agregado de destino.

2. Adicione os SSDs ao agregado usando o `storage aggregate add` comando.
   - Você pode especificar os SSDs por ID ou usando os `diskcount` parâmetros e. `disktype`
   - Se os HDDs e os SSDs não tiverem o mesmo tipo de checksum, ou se o agregado for um agregado de checksum misto, você deverá usar o `checksumstyle` parâmetro para especificar o tipo de checksum dos discos que você está adicionando ao agregado.
   - Você pode especificar um tipo RAID diferente para o cache SSD usando o `raidtype` parâmetro.
   - Se você quiser que o tamanho do grupo RAID de cache seja diferente do padrão para o tipo RAID que você está usando, você deve alterá-lo agora, usando o `-cache-raid-group-size` parâmetro.

Criar uma camada local (agregado) do Flash Pool usando pools de storage de SSD

Visão geral da criação de um nível local (agregado) do Flash Pool usando pools de storage SSD

Você pode executar vários procedimentos para criar uma camada local (agregada) do Flash Pool usando pools de storage SSD:

- **Preparação**
  - "Determine se uma camada local (agregado) do Flash Pool está usando um pool de storage SSD"
- * Criação de conjunto de armazenamento SSD*
  - "Crie um pool de armazenamento SSD"
  - "Adicione SSDs a um pool de armazenamento SSD"
- * Criação do Flash Pool usando pools de armazenamento SSD*
  - "Crie um nível local (agregado) do Flash Pool usando unidades de alocação do pool de storage SSD"
  - "Determine o impactos no tamanho do cache da adição de SSDs a um pool de armazenamento SSD"

Determine se uma camada local (agregado) do Flash Pool está usando um pool de storage SSD

Você pode configurar um agregado de Flash Pool (camada local) adicionando uma ou mais unidades de alocação de um pool de storage SSD a uma camada local de HDD existente.

Você gerencia as camadas locais do Flash Pool de maneira diferente quando eles usam pools de storage SSD para fornecer seu cache do que quando usam SSDs discretos.

Passo

1. Exibir as unidades do agregado por grupo RAID:

   `storage aggregate show-status` *`aggr_name`*

   Se o agregado estiver usando um ou mais pools de armazenamento SSD, o valor `Position` da coluna para os grupos RAID SSD será exibido como `Shared`, e o nome do pool de armazenamento será exibido ao lado do nome do grupo RAID.

Adicione cache a um nível local (agregado) criando um pool de storage SSD

Você pode provisionar o cache convertendo uma camada local (agregado) existente em uma camada local do Flash Pool (agregado) adicionando unidades de estado sólido (SSDs).

Você pode criar pools de storage de unidades de estado sólido (SSD) para fornecer cache SSD para duas a quatro camadas locais de Pool Flash (agregados). Agregados Flash Pool permitem que você implante flash como cache de alta performance para seu conjunto de dados em trabalho, ao mesmo tempo em que usa HDDs de baixo custo para dados acessados com menos frequência.

Sobre esta tarefa

- Você deve fornecer uma lista de discos ao criar ou adicionar discos a um pool de armazenamento.

  Os pools de armazenamento não suportam um `diskcount` parâmetro.

- Os SSDs usados no pool de storage devem ter o mesmo tamanho.

System Manager

Use o Gerenciador do sistema para adicionar um cache SSD (ONTAP 9.12,1 e posterior)

A partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para adicionar um cache SSD.

As opções de pool de storage não estão disponíveis em sistemas AFF.

Passos

1. Clique em **Cluster > Disks** e, em seguida, clique em **Show/Hide**.
2. Selecione **Type** e verifique se há SSDs sobressalentes no cluster.
3. Clique em **Storage > Tiers** e clique em **Add Storage Pool**.
4. Selecione o tipo de disco.
5. Introduza um tamanho de disco.
6. Selecione o número de discos a serem adicionados ao pool de armazenamento.
7. Reveja o tamanho estimado da cache.

Use o Gerenciador do sistema para adicionar um cache SSD (somente ONTAP 9.7)

Use o procedimento CLI se você estiver usando uma versão do ONTAP posterior ao ONTAP 9.7 ou anterior ao ONTAP 9.12,1.

Passos

1. Clique em **(retornar à versão clássica)**.
2. Clique em **armazenamento > agregados e discos > agregados**.
3. Selecione o nível local (agregado) e clique em **ações > Adicionar cache**.
4. Selecione a origem do cache como "pools de armazenamento" ou "SSDs dedicados".
5. Clique em **(mudar para a nova experiência)**.
6. Clique em **armazenamento > camadas** para verificar o tamanho do novo agregado.

CLI

Use a CLI para criar um pool de armazenamento SSD

Passos

1. Determine os nomes dos SSDs sobressalentes disponíveis:

   ```
   storage aggregate show-spare-disks -disk-type SSD
   ```

   Os SSDs usados em um pool de storage podem pertencer a qualquer nó de um par de HA.

2. Crie o pool de armazenamento:

   ```
   storage pool create -storage-pool sp_name -disk-list disk1,disk2,…
   ```

3. **Opcional:** Verifique o pool de armazenamento recém-criado:

```
storage pool show -storage-pool sp_name
```

Resultados

Depois que os SSDs são colocados no pool de storage, eles não aparecerão mais como sobressalentes no cluster, mesmo que o storage fornecido pelo pool de armazenamento ainda não tenha sido alocado a nenhum cache do Flash Pool. Não é possível adicionar SSDs a um grupo RAID como unidades discretas; o armazenamento deles pode ser provisionado somente usando as unidades de alocação do pool de armazenamento ao qual pertencem.

Crie um nível local (agregado) do Flash Pool usando unidades de alocação do pool de storage SSD

Você pode configurar um nível local (agregado) do Flash Pool adicionando uma ou mais unidades de alocação de um pool de storage SSD a um nível local de HDD existente.

A partir do ONTAP 9.12,1, você pode usar o Gerenciador de sistema reprojetado para criar um nível local de pool flash usando unidades de alocação de pool de storage.

O que você vai precisar

- Você precisa ter identificado um nível local válido composto de HDDs para converter em um nível local de Flash Pool.
- Você precisa ter determinado a qualificação para o armazenamento em cache de gravação dos volumes associados ao nível local e concluído as etapas necessárias para resolver problemas de qualificação.
- Você precisa criar um pool de storage SSD para fornecer o cache SSD a esse nível local do Flash Pool.

  Qualquer unidade de alocação do pool de storage que você deseja usar deve pertencer ao mesmo nó que possui a camada local do Flash Pool.

- Você deve ter determinado a quantidade de cache que deseja adicionar ao nível local.

  Você adiciona cache ao nível local por unidades de alocação. Você pode aumentar o tamanho das unidades de alocação posteriormente adicionando SSDs ao pool de armazenamento se houver espaço.

- Você deve ter determinado o tipo de RAID que deseja usar para o cache SSD.

  Depois de adicionar um cache ao nível local a partir de pools de armazenamento SSD, não é possível alterar o tipo RAID dos grupos RAID de cache.

- Você deve ter determinado o tamanho máximo de cache para o seu sistema e determinado que adicionar cache SSD ao seu nível local não fará com que você o exceda.

  Você pode ver a quantidade de cache que será adicionada ao tamanho total do cache usando o `storage pool show` comando.

- Você precisa se familiarizar com os requisitos de configuração do nível local do Flash Pool.

Sobre esta tarefa

Se pretender que o tipo RAID do cache seja diferente do dos grupos RAID do HDD, tem de especificar o tipo RAID do cache quando adicionar a capacidade do SSD. Depois de adicionar a capacidade SSD ao nível local, não é possível alterar mais o tipo RAID do cache.

Depois de adicionar um cache SSD a um nível local para criar um nível local do Flash Pool, não é possível

remover o cache SSD para converter o nível local de volta à configuração original.

System Manager

A partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para adicionar SSDs a um pool de armazenamento SSD.

Passos

1. Clique em **armazenamento > camadas** e selecione um nível de armazenamento HDD local existente.
2. Clique ⋮ e selecione **Add Flash Pool Cache**.
3. Selecione **Use Storage Pools**.
4. Selecione um pool de armazenamento.
5. Selecione um tamanho de cache e uma configuração RAID.
6. Clique em **Salvar**.
7. Localize a camada de storage novamente e clique ⋮em .
8. Selecione **mais detalhes** e verifique se o Flash Pool é exibido como **ativado**.

CLI

Passos

1. Marque o agregado como qualificado para se tornar um agregado de Flash Pool:

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   Se essa etapa não for bem-sucedida, determine a qualificação para o armazenamento em cache de gravação para o agregado de destino.

2. Mostrar as unidades de alocação de conjunto de armazenamento SSD disponíveis:

   ```
   storage pool show-available-capacity
   ```

3. Adicione a capacidade SSD ao agregado:

   ```
   storage aggregate add aggr_name -storage-pool sp_name -allocation-units
   number_of_units
   ```

   Se pretender que o tipo RAID do cache seja diferente do dos grupos RAID do HDD, tem de o alterar quando introduzir este comando utilizando o `raidtype` parâmetro.

   Não é necessário especificar um novo grupo RAID; o ONTAP coloca automaticamente o cache SSD em grupos RAID separados dos grupos RAID HDD.

   Não é possível definir o tamanho do grupo RAID do cache; ele é determinado pelo número de SSDs no pool de armazenamento.

   O cache é adicionado ao agregado e o agregado agora é um agregado de Flash Pool. Cada unidade de alocação adicionada ao agregado se torna seu próprio grupo RAID.

4. Confirme a presença e o tamanho do cache SSD:

   ```
   storage aggregate show aggregate_name
   ```

O tamanho do cache está listado em `Total Hybrid Cache Size`.

Informações relacionadas

"Relatório técnico da NetApp 4070: Guia de design e implementação de Flash Pool"

Determine o impactos no tamanho do cache da adição de SSDs a um pool de armazenamento SSD

Se a adição de SSDs a um pool de storage fizer com que o limite de cache do modelo de plataforma seja excedido, o ONTAP não alocará a capacidade recém-adicionada a nenhuma camada local (agregados) do Flash Pool. Isso pode resultar em que alguma ou toda a capacidade recém-adicionada não esteja disponível para uso.

Sobre esta tarefa

Quando você adiciona SSDs a um pool de storage SSD que tem unidades de alocação já alocadas a camadas locais (agregados) do Flash Pool, você aumenta o tamanho do cache de cada uma dessas camadas locais e o cache total no sistema. Se nenhuma das unidades de alocação do pool de armazenamento tiver sido alocada, adicionar SSDs a esse pool de armazenamento não afetará o tamanho do cache SSD até que uma ou mais unidades de alocação sejam alocadas a um cache.

Passos

1. Determine o tamanho utilizável dos SSDs que você está adicionando ao pool de storage:

   `storage disk show` *`disk_name`* `-fields usable-size`

2. Determine quantas unidades de alocação permanecem não alocadas para o pool de armazenamento:

   `storage pool show-available-capacity` *`sp_name`*

   Todas as unidades de alocação não alocadas no pool de armazenamento são exibidas.

3. Calcule a quantidade de cache que será adicionada aplicando a seguinte fórmula:

   (4 — número de unidades de alocação não alocadas) x 25% x tamanho utilizável x número de SSDs

Adicione SSDs a um pool de armazenamento SSD

Quando você adiciona unidades de estado sólido (SSDs) a um pool de armazenamento SSD, aumenta os tamanhos físicos e utilizáveis do pool de armazenamento e o tamanho da unidade de alocação. O tamanho maior da unidade de alocação também afeta as unidades de alocação que já foram alocadas a níveis locais (agregados).

O que você vai precisar

Você precisa ter determinado que essa operação não fará com que você exceda o limite de cache do seu par de HA. O ONTAP não impede que você exceda o limite de cache quando você adiciona SSDs a um pool de armazenamento SSD, e isso pode tornar a capacidade de armazenamento recém-adicionada indisponível para uso.

Sobre esta tarefa

Ao adicionar SSDs a um pool de storage SSD existente, os SSDs precisam pertencer a um nó ou a outro do mesmo par de HA que já possuía os SSDs existentes no pool de storage. Você pode adicionar SSDs de

propriedade de qualquer nó do par de HA.

O SSD que você adicionar ao pool de armazenamento deve ter o mesmo tamanho do disco usado no pool de armazenamento.

System Manager

A partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para adicionar SSDs a um pool de armazenamento SSD.

Passos

1. Clique em **armazenamento > camadas** e localize a seção **conjuntos de armazenamento**.
2. Localize o pool de armazenamento, clique em e selecione **Adicionar discos**.
3. Escolha o tipo de disco e selecione o número de discos.
4. Reveja o tamanho do cache estimado.

CLI

Passos

1. **Opcional:** Veja o tamanho atual da unidade de alocação e o armazenamento disponível para o pool de armazenamento:

   `storage pool show -instance` *`sp_name`*

2. Encontre SSDs disponíveis:

   `storage disk show -container-type spare -type SSD`

3. Adicione os SSDs ao pool de storage:

   `storage pool add -storage-pool sp_name -disk-list` *`disk1,disk2…`*

   O sistema exibe quais agregados Flash Pool terão seu tamanho aumentado por essa operação e por quanto, e solicita que você confirme a operação.

Comandos para gerenciar pools de storage SSD

O ONTAP fornece o `storage pool` comando para gerenciar pools de storage SSD.

Se você quiser…	Use este comando…
Mostrar a quantidade de storage que um pool de storage está fornecendo a quais agregados	`storage pool show-aggregate`
Exibir quanto cache seria adicionado à capacidade geral de cache para ambos os tipos de RAID (tamanho de dados da unidade de alocação)	`storage pool show -instance`
Exibir os discos em um pool de armazenamento	`storage pool show-disks`

Exibir as unidades de alocação não alocadas para um pool de armazenamento	`storage pool show-available-capacity`
Alterar a propriedade de uma ou mais unidades de alocação de um pool de storage de um parceiro de HA para outro	`storage pool reassign`

Informações relacionadas

- "Referência do comando ONTAP"

Gerenciamento de nível FabricPool

Saiba mais sobre a disposição de dados em camadas com o ONTAP FabricPool

Você pode usar o FabricPool para categorizar dados automaticamente, dependendo da frequência com que os dados são acessados.

O FabricPool é uma solução de storage híbrido que, nos sistemas AFF, usa um agregado all-flash (SSD) e, nos sistemas FAS, usa um agregado all-flash (SSD) ou HDD como a categoria de performance e um armazenamento de objetos como a camada de nuvem. O uso de um FabricPool ajuda a reduzir os custos de storage sem comprometer a performance, a eficiência ou a proteção.

A categoria de nuvem pode estar localizada no NetApp StorageGRID ou no ONTAP S3 (a partir do ONTAP 9.8) ou em um dos seguintes fornecedores de serviços:

- Alibaba nuvem
- Amazon S3
- Amazon Commercial Cloud Services
- Google Cloud
- Nuvem da IBM
- Storage Blob do Microsoft Azure

> A partir do ONTAP 9.7, provedores de armazenamento de objetos adicionais que suportam APIs S3 genéricas podem ser usados selecionando o provedor de armazenamento de objetos S3_compatible.

Informações relacionadas

Consulte também a "Disposição em camadas na nuvem do NetApp" documentação.

Requisitos para usar o ONTAP FabricPool

Para ajudar a garantir que você otimize suas configurações do FabricPool, você deve se familiarizar com algumas considerações e requisitos sobre o uso do FabricPool.

Considerações gerais e requisitos

ONTAP 9,2

Você deve estar executando o ONTAP 9.2 ou posterior FabricPool.

ONTAP 9,4

- Você deve estar executando o ONTAP 9.4 ou versões posteriores para a seguinte funcionalidade do FabricPool:
  - O `auto` "política de disposição em camadas"
  - Especificando o período mínimo de resfriamento em camadas
  - Relatório de dados inativos (IDR)
  - Uso do storage de Blob do Microsoft Azure para a nuvem como a categoria de nuvem do FabricPool
  - Usando o FabricPool com ONTAP Select

ONTAP 9,5

- Você deve estar executando o ONTAP 9.5 ou versões posteriores para a seguinte funcionalidade do FabricPool:
  - Especificando o limite de preenchimento de disposição em camadas
  - Uso do IBM Cloud Object Storage como camada de nuvem do FabricPool
  - Criptografia de volume NetApp (NVE) da camada de nuvem, habilitada por padrão.

ONTAP 9,6

- Você deve estar executando o ONTAP 9.6 ou versões posteriores para a seguinte funcionalidade do FabricPool:
  - A `all` política de disposição em camadas
  - Relatórios de dados inativos ativados manualmente em agregados HDD
  - Relatórios de dados inativos ativados automaticamente para agregados SSD quando você atualiza para o ONTAP 9.6 e, no momento, o agregado é criado, exceto em sistemas low-end com menos de 4 CPUs, menos de 6 GB de RAM, ou quando o tamanho do cache de buffer WAFL é inferior a 3 GB.

    O ONTAP monitora a carga do sistema e, se a carga permanecer alta por 4 minutos contínuos, o IDR é desativado e não é ativado automaticamente. Você pode reativar o IDR manualmente, no entanto, o IDR ativado manualmente não é desativado automaticamente.

  - Usar o storage de objetos na nuvem Alibaba como camada de nuvem para FabricPool
  - Uso do Google Cloud Platform como camada de nuvem do FabricPool
  - Movimentação de volumes sem cópia de dados de categoria de nuvem

ONTAP 9,7

- Você deve estar executando o ONTAP 9.7 ou versões posteriores para a seguinte funcionalidade do FabricPool:
  - Proxy HTTP e HTTPS não transparente para fornecer acesso apenas a pontos de acesso em branco e para fornecer recursos de auditoria e relatórios.
  - Espelhamento FabricPool para categorizar dados inativos em dois armazenamentos de objetos simultaneamente

- Espelhos FabricPool nas configurações do MetroCluster
- Despejo de NDMP e restauração ativados por padrão em agregados conetados ao FabricPool.

> Se a aplicação de backup usar um protocolo diferente do NDMP, como NFS ou SMB, todos os dados que estiverem sendo copiados na categoria de performance aquecem e podem afetar a disposição em camadas desses dados na categoria de nuvem. Leituras não NDMP podem causar a migração de dados da camada de nuvem de volta para a camada de performance.

"Suporte de backup e restauração NDMP para FabricPool"

ONTAP 9,8

- Você deve estar executando o ONTAP 9.8 ou posterior para a seguinte funcionalidade do FabricPool:
  - Recuperação da nuvem
  - FabricPool com SnapLock Enterprise. O FabricPool com SnapLock Enterprise requer uma solicitação de variação de produto (FPVR). Para criar um FPVR, entre em Contato com sua equipe de vendas.
  - Período mínimo de resfriamento máximo de 183 dias
  - Marcação de objetos usando tags personalizadas criadas pelo usuário
  - Agregados HDD FabricPool

    HDD FabricPools são suportados com discos SAS, FSAS, BSAS e MSATA somente em sistemas com 6 ou mais núcleos de CPU.

Verifique "Hardware Universe" se existem os modelos suportados mais recentes.

ONTAP 9.10,1

- Você deve estar executando o ONTAP 9.10,1 ou posterior para a seguinte funcionalidade do FabricPool:
  - COLOQUE estrangulamento
  - Eficiência de armazenamento sensível à temperatura (TSSE).

ONTAP 9.12,1

- Você deve estar executando o ONTAP 9.12,1 ou posterior para a seguinte funcionalidade do FabricPool:
  - Migração da SVM
  - Suporte para FabricPool, FlexGroup e SVM-DR trabalhando em conjunto. (Antes de 9.12.1, quaisquer dois desses recursos trabalharam juntos, mas nem todos os três em conjunto.)

ONTAP 9.14,1

- Você deve estar executando o ONTAP 9.14,1 ou posterior para a seguinte funcionalidade do FabricPool:
  - Gravação na nuvem
  - Preparação agressiva

Camadas locais (agregados)

O FabricPool oferece suporte aos seguintes tipos de agregados:

- Em sistemas AFF, você só pode usar agregados SSD para FabricPool.
- Em sistemas FAS, você pode usar agregados SSD ou HDD para FabricPool.
- No Cloud Volumes ONTAP e no ONTAP Select, você pode usar agregados SSD ou HDD para FabricPool. Recomenda-se o uso de agregados SSD.

Agregados Flash Pool, que contêm SSDs e HDDs, não são compatíveis.

Categorias de nuvem

O FabricPool é compatível com o uso dos seguintes armazenamentos de objetos como a camada de nuvem:

- Alibaba Cloud Object Storage Service (padrão, acesso não frequente)
- Amazon S3 (Standard, Standard-IA, One Zone-IA, Intelligent-Tiering, Glacier Instant Retrieval)
- Serviços de nuvem comerciais da Amazon (C2S)
- Google Cloud Storage (Multi-Regional, Regional, Nearline, Coldline, Archive)
- IBM Cloud Object Storage (padrão, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (ativo e inativo)
- NetApp ONTAP S3 (ONTAP 9 .8 e posterior)
- NetApp StorageGRID (StorageGRID 10,3 e posterior)

O Glacier Flexible Retrieval e o Glacier Deep Archive não são suportados.

- O repositório de objetos "'bucket'" (contentor) que você pretende usar deve já ter sido configurado, deve ter pelo menos 10 GB de espaço de armazenamento e não deve ser renomeado.
- Os pares DE HA que usam FabricPool exigem LIFs entre clusters para se comunicar com o armazenamento de objetos.
- Não é possível separar um nível de nuvem de um nível local depois que ele é anexado. No entanto, é possível "Espelho FabricPool"anexar um nível local a um nível de nuvem diferente.

Eficiência de storage da ONTAP

Preservamos eficiências de storage, como compressão, deduplicação e compactação, ao mover dados para a camada de nuvem, reduzindo a capacidade de storage de objetos e os custos de transporte necessários.

A partir do ONTAP 9.15,1, o FabricPool suporta a tecnologia Intel QuickAssist (QAT4), que proporciona uma economia de eficiência de armazenamento mais agressiva e com melhor desempenho.

A deduplicação in-line agregada é compatível com a categoria local, mas as eficiências de storage associadas não são transferidas para objetos armazenados na categoria de nuvem.

Ao usar a política de disposição em categorias de todos os volumes, as eficiências de storage associadas aos processos de deduplicação em segundo plano podem ser reduzidas, pois é provável que os dados sejam dispostos em camadas antes da aplicação das eficiências de storage adicionais.

Licença de disposição em camadas do BlueXP

O FabricPool requer uma licença baseada em capacidade ao anexar fornecedores de storage de objetos de terceiros (como Amazon S3) como camadas de nuvem para sistemas AFF e FAS. Não é necessária uma licença de disposição em camadas do BlueXP ao usar o StorageGRID ou o ONTAP S3 como camada de nuvem ou ao dispor em camadas no Cloud Volumes ONTAP, no Amazon FSX for NetApp ONTAP ou no Azure NetApp Files.

As licenças BlueXP (incluindo suplementos ou extensões para licenças FabricPool pré-existentes) são ativadas no "Carteira digital BlueXP".

Controles de consistência do StorageGRID

Os controles de consistência do StorageGRID afetam a forma como os metadados que o StorageGRID usa para rastrear objetos são distribuídos entre nós e a disponibilidade de objetos para solicitações de clientes. A NetApp recomenda usar o controle de consistência padrão, leitura após nova gravação, para buckets usados como destinos do FabricPool.

Não use o controle de consistência disponível para buckets usados como alvos FabricPool.

Considerações adicionais para disposição em camadas de dados acessados por protocolos SAN

Ao dispor em camadas os dados acessados por protocolos SAN, a NetApp recomenda o uso de nuvens privadas, como o ONTAP S3 ou o StorageGRID, devido a considerações de conectividade.

Você deve estar ciente de que ao usar o FabricPool em um ambiente SAN com um host Windows, se o armazenamento de objetos ficar indisponível por um período prolongado de tempo ao categorizar dados na nuvem, os arquivos no LUN NetApp no host do Windows podem ficar inacessíveis ou desaparecer. Consulte o artigo da base de dados de Conhecimento "Durante o armazenamento de objetos do FabricPool S3 não disponível, o host do Windows SAN relatou corrupção do sistema de arquivos".

Qualidade do serviço

- Se você usar andares de taxa de transferência (QoS min), a política de disposição em categorias nos volumes deve ser definida como `none` antes que o agregado possa ser anexado ao FabricPool.

  Outras políticas de disposição em camadas impedem que o agregado seja anexado ao FabricPool. Uma política de QoS não irá impor pisos de taxa de transferência quando o FabricPool estiver ativado.

Funcionalidade ou recursos não suportados pelo FabricPool

- Armazenamentos de objetos com WORM ativado e controle de versão de objetos habilitado.
- Políticas de gerenciamento do ciclo de vida das informações (ILM) aplicadas aos buckets do armazenamento de objetos

  O FabricPool é compatível com as políticas de gerenciamento do ciclo de vida das informações da StorageGRID apenas para replicação de dados e codificação de apagamento a fim de proteger os dados da camada de nuvem contra falhas. No entanto, o FabricPool *não* suporta regras avançadas de ILM, como filtragem baseada em metadados ou tags do usuário. O ILM geralmente inclui várias políticas de movimento e exclusão. Essas políticas podem causar interrupções nos dados na camada de nuvem do FabricPool. Usar o FabricPool com políticas ILM configuradas em armazenamentos de objetos pode resultar em perda de dados.

- Transição de dados de 7 modos usando os comandos CLI do ONTAP ou a ferramenta de transição de 7 modos
- Virtualização FlexArray
- RAID SyncMirror, exceto em uma configuração MetroCluster
- Volumes do SnapLock ao usar o ONTAP 9.7 e versões anteriores
- Backup em fita usando SMTape para agregados habilitados para FabricPool
- A funcionalidade de equilíbrio automático
- Volumes que utilizam uma garantia de espaço diferente de `none`

  Com a exceção dos volumes raiz da SVM e dos volumes de preparação de auditoria CIFS, o FabricPool não é compatível com a inclusão de uma camada de nuvem a um agregado que contenha volumes usando uma garantia de espaço diferente `none`do . Por exemplo, um volume usando uma garantia de espaço `volume` (`-space-guarantee` `volume`do) não é suportado.

- Clusters com "Licença DP_otimizada"
- Agregados Flash Pool

Armazene dados em categorias de forma eficiente com as políticas do ONTAP FabricPool

As políticas de disposição em camadas do FabricPool permitem que você mova dados com eficiência entre camadas à medida que os dados ficam inativos. Compreender as políticas de disposição em camadas ajuda você a selecionar a política certa que atende às suas necessidades de gerenciamento de storage.

Tipos de políticas de disposição em camadas do FabricPool

As políticas de disposição em camadas do FabricPool determinam quando ou se os blocos de dados do usuário de um volume no FabricPool são movidos para a camada de nuvem, com base na temperatura do volume de quente (ativo) ou frio (inativo). O volume "temperatura" aumenta quando é acessado com frequência e diminui quando não é. Algumas políticas de disposição em camadas têm um período de resfriamento mínimo de disposição em camadas associado, que define o tempo em que os dados do usuário em um volume de FabricPool precisam permanecer inativos para que os dados sejam considerados "inativos" e movidos para a camada de nuvem.

Depois que um bloco foi identificado como frio, ele é marcado como elegível para ser escalonado. Uma verificação diária em camadas de fundo procura blocos frios. Quando suficientes blocos 4KB do mesmo volume forem coletados, eles são concatenados em um objeto 4MB e movidos para a camada de nuvem com base na política de disposição em categorias de volume.

> Os dados em volumes que usam a `all` política de disposição em camadas são imediatamente marcados como inativos e começam a categorização na categoria de nuvem o mais rápido possível. Não é necessário esperar que a digitalização de disposição em camadas diária seja executada.

Você pode usar o[`volume object-store tiering show` comando para exibir o status de disposição em camadas de um volume FabricPool. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//volume-object-store-tiering-show.html[`volume object-store tiering show`em referência de comando ONTAP.

A política de disposição em camadas do FabricPool é especificada no nível do volume. Estão disponíveis quatro opções:

- A `snapshot-only` política de disposição em camadas (padrão) move blocos de dados do usuário das cópias do Snapshot de volume que não estão associados ao sistema de arquivos ativo para a camada de nuvem.

  O período mínimo de resfriamento em categorias é de 2 dias. É possível modificar a configuração padrão para o período mínimo de resfriamento em camadas com o `-tiering-minimum-cooling-days` parâmetro no nível de privilégio avançado dos `volume create` comandos e. `volume modify` Os valores válidos são de 2 a 183 dias usando o ONTAP 9.8 e posterior. Se você estiver usando uma versão do ONTAP anterior a 9,8, os valores válidos são de 2 a 63 dias.

- A `auto` política de disposição em camadas, compatível apenas com o ONTAP 9.4 e versões posteriores, move blocos de dados de usuários inativos nas cópias Snapshot e no sistema de arquivos ativo para a camada de nuvem.

  O período de resfriamento mínimo de disposição em camadas padrão é de 31 dias e aplica-se a todo o volume, tanto para o sistema de arquivos ativo quanto para as cópias Snapshot.

  É possível modificar a configuração padrão para o período mínimo de resfriamento em camadas com o `-tiering-minimum-cooling-days` parâmetro no nível de privilégio avançado dos `volume create` comandos e. `volume modify` Os valores válidos são de 2 a 183 dias.

- `all`A política de disposição em camadas, compatível apenas com o ONTAP 9.6 e posterior, move todos os blocos de dados de usuários no sistema de arquivos ativo e cópias Snapshot para a camada de nuvem. Ele substitui a `backup` política de disposição em camadas.

  A `all` política de disposição em categorias de volume não deve ser usada em volumes de leitura/gravação que tenham tráfego de cliente normal.

  O período de resfriamento mínimo de disposição em camadas não se aplica porque os dados são movidos para a camada de nuvem assim que a verificação de disposição em camadas é executada e não é possível modificar a configuração.

- A `none` política de disposição em categorias mantém os dados de um volume na categoria de performance e não é migrada para a camada de nuvem.

  Definir a política de disposição em categorias `none` para impedir a nova disposição em camadas. Os dados de volume anteriormente movidos para a camada de nuvem permanecem na camada de nuvem até que fiquem ativos e são movidos automaticamente de volta para a camada local.

  O período de resfriamento mínimo de disposição em camadas não se aplica porque os dados nunca são movidos para a camada de nuvem e não é possível modificar a configuração.

  Quando blocos frios em um volume com uma política de disposição em categorias definida como `none` são lidos, eles ficam ativos e gravados no nível local.

O `volume show` comando output mostra a política de disposição em camadas de um volume. Um volume que nunca foi usado com o FabricPool mostra a `none` política de disposição em camadas na saída.

O que acontece quando você modifica a política de disposição em camadas de um volume no FabricPool

Você pode modificar a política de disposição em categorias de um volume executando `volume modify` uma operação. Você deve entender como mudar a política de disposição em camadas pode afetar o tempo necessário para que os dados fiquem inativos e sejam movidos para a categoria de nuvem.

- Ao alterar a política de disposição em categorias de `snapshot-only` ou `none` para `auto`, o ONTAP pode enviar blocos de dados de usuários no sistema de arquivos ativo que já estão inativos na categoria de nuvem, mesmo que esses blocos de dados de usuários não estivessem qualificados anteriormente para a categoria de nuvem.
- A alteração da política de disposição em camadas para `all` outra política faz com que o ONTAP mova todos os blocos de usuários no sistema de arquivos ativo e nas cópias Snapshot para a nuvem o mais rápido possível. Antes do ONTAP 9.8, os blocos precisavam esperar até que a próxima verificação de disposição em camadas fosse executada.

  Mover blocos de volta para o nível de desempenho não é permitido.

- Alterar a política de disposição em categorias de `auto` ou `none` para `snapshot-only` fazer com que os blocos de sistema de arquivos ativos que já foram migrados para a categoria de nuvem sejam movidos de volta para a categoria de performance.

  Leituras de volume são necessárias para que os dados sejam movidos de volta para a camada de performance.

- Sempre que você alterar a política de disposição em categorias em um volume, o período mínimo de resfriamento em categorias será redefinido para o valor padrão da política.

O que acontece com a política de disposição em camadas quando você move um volume

- A menos que você especifique explicitamente uma política de disposição em camadas diferente, um volume mantém sua política de disposição em camadas original quando é movido para dentro e para fora de um agregado habilitado para FabricPool.

  No entanto, a política de disposição em categorias só entra em vigor quando o volume está em um agregado habilitado para FabricPool.

- O valor existente `-tiering-minimum-cooling-days` do parâmetro para um volume é movido com o volume, a menos que você especifique uma política de disposição em camadas diferente para o destino.

  Se você especificar uma política de disposição em camadas diferente, o volume usará o período mínimo de resfriamento de disposição em camadas padrão para essa política. Este é o caso se o destino é FabricPool ou não.

- Você pode mover um volume entre agregados e, ao mesmo tempo, modificar a política de disposição em camadas.
- Você deve prestar atenção especial quando `volume move` uma operação envolver a `auto` política de disposição em camadas.

  Supondo que a origem e o destino sejam agregados habilitados para FabricPool, a tabela a seguir resume o resultado de uma `volume move` operação que envolve alterações de política relacionadas `auto` ao :

Quando você move um volume que tem uma política de disposição em camadas de…	E você altera a política de disposição em camadas com a…	Então, depois que o volume se move…
`all`	`auto`	Todos os dados são movidos para o nível de performance.
`snapshot-only`, `none`, ou `auto`	`auto`	Os blocos de dados são movidos para o mesmo nível de destino que anteriormente estavam na origem.
`auto` ou `all`	`snapshot-only`	Todos os dados são movidos para o nível de performance.
`auto`	`all`	Todos os dados de usuário são movidos para a camada de nuvem.
`snapshot-only`,`auto` ou `all`	`none`	Todos os dados são mantidos na camada de performance.

O que acontece com a política de disposição em camadas quando você clonar um volume

- A partir do ONTAP 9.8, um volume de clone herda sempre a política de disposição em camadas e a política de recuperação de nuvem do volume pai.

  Em versões anteriores ao ONTAP 9.8, um clone herda a política de disposição em camadas do pai, exceto quando o pai tem a `all` política de disposição em camadas.

- Se o volume pai tiver a `never` política de recuperação de nuvem, seu volume clone precisará ter a `never` política de recuperação de nuvem ou a `all` política de disposição em camadas e uma política de recuperação de nuvem correspondente `default` .
- A política de recuperação de nuvem de volume pai não pode ser alterada para `never`, a menos que todos os seus volumes clones tenham uma política de recuperação de `never` nuvem .

Ao clonar volumes, tenha em mente as seguintes práticas recomendadas:

- A `-tiering-policy` opção e `tiering-minimum-cooling-days` a opção do clone controlam apenas o comportamento de disposição em camadas de blocos exclusivos do clone. Portanto, recomendamos o uso de configurações de disposição em categorias no FlexVol pai que migram a mesma quantidade de dados ou que migram menos dados do que qualquer um dos clones
- A política de recuperação de nuvem no FlexVol pai deve mover a mesma quantidade de dados ou mover mais dados do que a política de recuperação de qualquer um dos clones

Como as políticas de disposição em camadas funcionam com a migração para a nuvem

A recuperação de dados em nuvem do FabricPool é controlada por políticas de disposição em camadas que determinam a recuperação de dados da camada de nuvem para a camada de performance com base no padrão de leitura. Os padrões de leitura podem ser sequenciais ou aleatórios.

A tabela a seguir lista as políticas de disposição em camadas e as regras de recuperação de dados na nuvem para cada política.

Política de disposição em camadas	Comportamento de recuperação
nenhum	Leituras sequenciais e aleatórias
apenas snapshot	Leituras sequenciais e aleatórias
auto	Leituras aleatórias
tudo	Sem recuperação de dados

A partir do ONTAP 9.8, a opção de controle de migração para a `cloud-retrieval-policy` nuvem substitui o comportamento padrão de migração ou recuperação da nuvem controlado pela política de disposição em camadas.

A tabela a seguir lista as políticas de recuperação de nuvem suportadas e seu comportamento de recuperação.

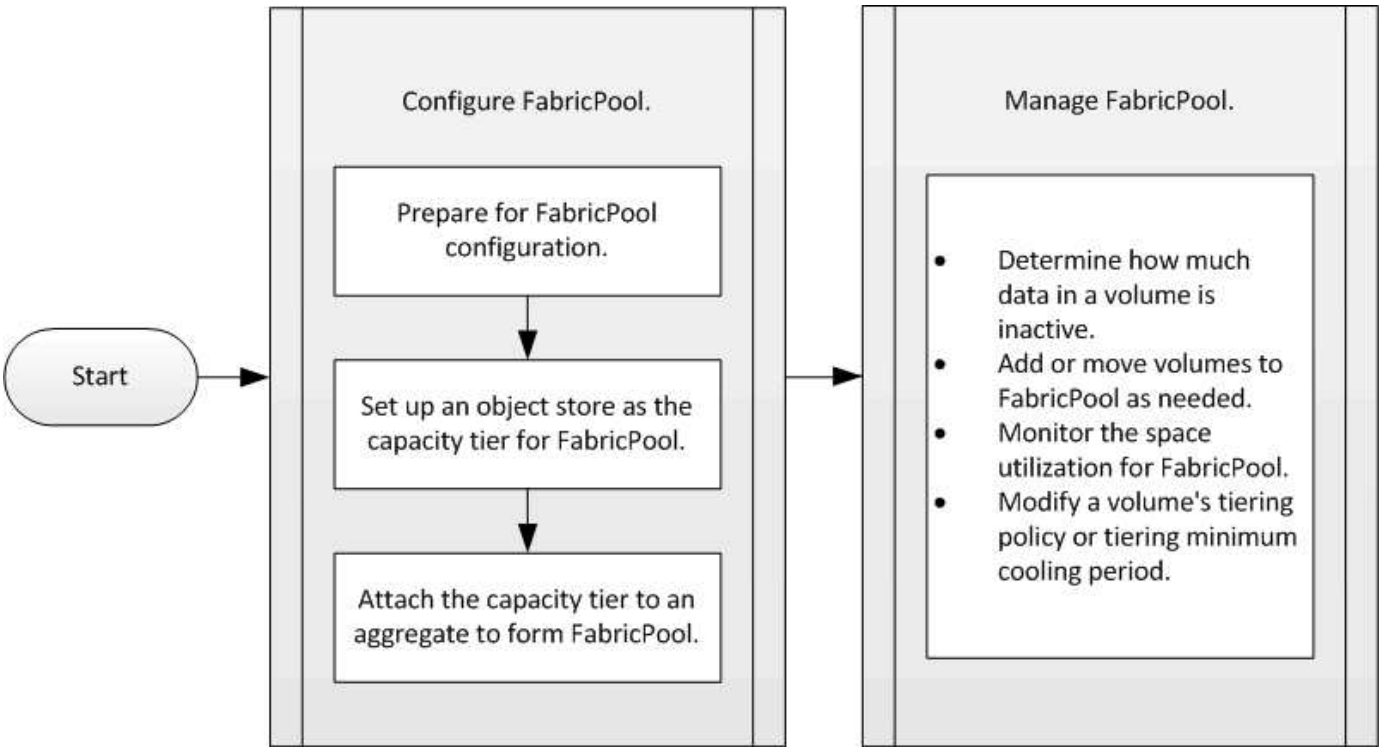
Política de recuperação de nuvem	Comportamento de recuperação
padrão	A política de disposição em camadas decide quais dados devem ser retirados, portanto, não há alteração na recuperação de dados na nuvem com "falha,`" `cloud-retrieval-policy`". Esta política é o valor padrão para qualquer volume, independentemente do tipo de agregado hospedado.
na leitura	Todas as leituras de dados orientadas pelo cliente são extraídas da camada de nuvem para a camada de performance.
nunca	Nenhum dado orientado pelo cliente é extraído da camada de nuvem para a camada de performance
promover	• Para a política de disposição em categorias "nenhuma", todos os dados de nuvem são extraídos da camada de nuvem para a camada de performance • Para a política de disposição em camadas "somente snapshot", os dados do AFS são extraídos.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Fluxo de trabalho de gerenciamento do FabricPool

Você pode usar o diagrama de fluxo de trabalho do FabricPool para ajudá-lo a Planejar

as tarefas de configuração e gerenciamento.



Configurar o FabricPool

Prepare-se para a configuração do FabricPool

Comece a usar o ONTAP FabricPool

A configuração do FabricPool ajuda a gerenciar qual camada de storage (a camada de performance local ou a camada de nuvem) os dados devem ser armazenados com base no fato de que eles são acessados com frequência.

A preparação necessária para a configuração do FabricPool depende do armazenamento de objetos que você usa como camada de nuvem.

Instale uma licença FabricPool em um cluster do ONTAP

A licença FabricPool que você pode ter usado no passado está mudando e está sendo mantida apenas para configurações que não são suportadas no BlueXP . A partir de 21 de agosto de 2021, o licenciamento BYOL do Cloud Tiering foi introduzido para configurações de disposição em camadas compatíveis com o BlueXP usando o serviço Cloud Tiering. A licença BYOL do Cloud Tiering agora é conhecida como a licença de disposição em camadas do BlueXP .

"Saiba mais sobre o licenciamento BYOL do BlueXP Cloud Tiering".

As configurações compatíveis com o BlueXP devem usar a página carteira digital no BlueXP para licenciar a disposição em camadas para clusters do ONTAP. Isso exige que você configure uma conta do BlueXP e configure a disposição em camadas para o fornecedor de storage de objetos específico que você planeja usar. Atualmente, o BlueXP oferece suporte à disposição em camadas no seguinte storage de objetos: Amazon S3,

storage Blob do Azure, Google Cloud Storage, storage de objetos compatível com S3 e StorageGRID.

"Saiba mais sobre o serviço Cloud Tiering".

Você pode baixar e ativar uma licença FabricPool usando o Gerenciador de sistema se tiver uma das configurações que não é suportada no BlueXP :

- Instalações do ONTAP em locais escuros
- ONTAP clusters que estão categorizando dados no IBM Cloud Object Storage ou Alibaba Cloud Object Storage

A licença FabricPool é uma licença de todo o cluster. Isso inclui um limite de uso adquirido para storage de objetos associado ao FabricPool no cluster. A utilização no cluster não deve exceder a capacidade do limite de utilização autorizado. Se você precisar aumentar o limite de uso da licença, entre em Contato com seu representante de vendas.

As licenças FabricPool estão disponíveis em formatos perpétuos ou baseados em termos de prazo, 1 ou 3 anos.

Uma licença FabricPool baseada em termos de 10 TB de capacidade gratuita está disponível para pedidos FabricPool pela primeira vez para configurações de clusters existentes não compatíveis com o BlueXP . A capacidade gratuita não está disponível com licenças perpétuas. Não é necessária uma licença se você usar o NetApp StorageGRID ou o ONTAP S3 para a camada de nuvem. O Cloud Volumes ONTAP não requer uma licença FabricPool, independentemente do fornecedor que está a utilizar.

Esta tarefa é suportada apenas carregando o ficheiro de licença para o cluster utilizando o System Manager.

Passos

1. Transfira o ficheiro de licença NetApp (NLF) para obter a licença FabricPool a partir do "Site de suporte da NetApp".
2. Execute as seguintes ações usando o Gerenciador do sistema para carregar a licença do FabricPool para o cluster:
   a. No painel **Cluster > Settings**, no cartão **Licenses**, clique em .
   b. Na página **Licença**, clique em .
   c. Na caixa de diálogo **Add License** (Adicionar licença), clique em **Browse** (Procurar) para selecionar o NLF transferido e, em seguida, clique em **Add** (Adicionar) para carregar o ficheiro para o cluster.

Informações relacionadas

"Visão geral do licenciamento do ONTAP FabricPool (FP)"

"Pesquisa de licença de software NetApp"

"NetApp TechComm TV: Lista de reprodução do FabricPool"

Instale um certificado de CA em um cluster do ONTAP para StorageGRID

O uso de certificados CA cria uma relação confiável entre aplicativos clientes e StorageGRID.

A menos que você Planeje desabilitar a verificação de certificados para o StorageGRID, você deve instalar um certificado da CA StorageGRID no cluster para que o ONTAP possa se autenticar com o StorageGRID como o armazenamento de objetos para o FabricPool.

Embora o StorageGRID possa gerar certificados autoassinados, o uso de certificados assinados de uma autoridade de certificação de terceiros é a prática recomendada.

Sobre esta tarefa

Embora a instalação e o uso de certificados de autoridade de certificação (CA) sejam práticas recomendadas, a partir do ONTAP 9.4, a instalação de certificados de CA não é necessária para o StorageGRID.

Passos

1. Contacte o administrador do StorageGRID para obter o "Certificado CA do sistema StorageGRID".
2. Use o `security certificate install` comando com o `-type server-ca` parâmetro para instalar o certificado da CA do StorageGRID no cluster.

   O nome de domínio totalmente qualificado (FQDN) inserido deve corresponder ao nome comum personalizado no certificado da CA do StorageGRID.

Atualizar um certificado expirado

Para atualizar um certificado expirado, a prática recomendada é usar uma CA confiável para gerar o novo certificado de servidor. Além disso, você deve garantir que o certificado seja atualizado no servidor StorageGRID e no cluster ONTAP ao mesmo tempo para manter qualquer tempo de inatividade ao mínimo.

Informações relacionadas

"Recursos do StorageGRID"

Instale um certificado de CA em um cluster para o ONTAP S3

O uso de certificados de CA cria uma relação confiável entre aplicativos clientes e o servidor de armazenamento de objetos ONTAP S3. Um certificado de CA deve ser instalado no ONTAP antes de usá-lo como um armazenamento de objetos acessível a clientes remotos.

A menos que você Planeje desabilitar a verificação de certificados para o ONTAP S3, você deve instalar um certificado de CA ONTAP S3 no cluster para que o ONTAP possa se autenticar com o ONTAP S3 como o armazenamento de objetos para o FabricPool.

Embora o ONTAP possa gerar certificados autoassinados, o uso de certificados assinados de uma autoridade de certificação de terceiros é a prática recomendada.

Passos

1. Obtenha o certificado CA do sistema ONTAP S3.
2. Use o `security certificate install` comando com o `-type server-ca` parâmetro para instalar o certificado da CA ONTAP S3 no cluster.

   O nome de domínio totalmente qualificado (FQDN) inserido deve corresponder ao nome comum personalizado no certificado de CA ONTAP S3.

Atualizar um certificado expirado

Para atualizar um certificado expirado, a prática recomendada é usar uma CA confiável para gerar o novo certificado de servidor. Além disso, você deve garantir que o certificado seja atualizado no servidor ONTAP S3 e no cluster ONTAP ao mesmo tempo para manter qualquer tempo de inatividade no mínimo.

Informações relacionadas

"Configuração S3"

Configure um armazenamento de objetos como a camada de nuvem do FabricPool

Configure um armazenamento de objetos como a camada de nuvem para a visão geral do FabricPool

A configuração do FabricPool envolve a especificação das informações de configuração do armazenamento de objetos (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage ou Microsoft Azure Blob Storage para a nuvem) que você planeja usar como a camada de nuvem do FabricPool.

Configure o StorageGRID como a camada de nuvem do ONTAP FabricPool

Se você estiver executando o ONTAP 9.2 ou posterior, poderá configurar o StorageGRID como a categoria de nuvem para o FabricPool. Ao dispor em camadas os dados acessados por protocolos SAN, a NetApp recomenda o uso de nuvens privadas, como o StorageGRID, devido a considerações de conectividade.

Considerações para usar o StorageGRID com FabricPool

- Você precisa instalar um certificado de CA para StorageGRID, a menos que você desative explicitamente a verificação de certificado.
- Você não deve habilitar o controle de versão de objetos do StorageGRID no bucket do armazenamento de objetos.
- Não é necessária uma licença FabricPool.
- Se um nó StorageGRID for implantado em uma máquina virtual com storage atribuído a partir de um sistema NetApp AFF, confirme se o volume não tem uma política de disposição em camadas do FabricPool ativada.

  A desativação da disposição em camadas do FabricPool para volumes usados com nós do StorageGRID simplifica a solução de problemas e as operações de storage.

> Nunca use o FabricPool para categorizar dados relacionados ao StorageGRID de volta ao próprio StorageGRID. A disposição em camadas de dados do StorageGRID de volta para o StorageGRID aumenta a complexidade operacional e a solução de problemas.

Sobre esta tarefa

O balanceamento de carga está habilitado para StorageGRID no ONTAP 9.8 e posterior. Quando o nome do host do servidor resolve mais de um endereço IP, o ONTAP estabelece conexões de cliente com todos os endereços IP retornados (até um máximo de 16 endereços IP). Os endereços IP são coletados em um método round-robin quando as conexões são estabelecidas.

Procedimentos

Você pode configurar o StorageGRID como a categoria de nuvem para o FabricPool com o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

System Manager

1. Clique em **armazenamento > camadas > Adicionar nível de nuvem** e selecione StorageGRID como o provedor de armazenamento de objetos.
2. Preencha as informações solicitadas.
3. Se você quiser criar um espelho na nuvem, clique em **Adicionar como espelho FabricPool**.

Um espelhamento do FabricPool fornece um método para você substituir perfeitamente um armazenamento de dados e ajuda a garantir que seus dados estejam disponíveis em caso de desastre.

CLI

1. Especifique as informações de configuração do StorageGRID usando o `storage aggregate object-store config create` comando com o `-provider-type SGWS` parâmetro.
   - O `storage aggregate object-store config create` comando falhará se o ONTAP não puder acessar o StorageGRID com as informações fornecidas.
   - Use o `-access-key` parâmetro para especificar a chave de acesso para autorizar solicitações ao armazenamento de objetos StorageGRID.
   - Use o `-secret-password` parâmetro para especificar a senha (chave de acesso secreto) para autenticar solicitações no armazenamento de objetos StorageGRID.
   - Se a senha do StorageGRID for alterada, você deve atualizar a senha correspondente armazenada no ONTAP imediatamente.

     Com isso, o ONTAP pode acessar os dados no StorageGRID sem interrupção.
   - Definir o `-is-certificate-validation-enabled` parâmetro para `false` desativa a verificação de certificados para StorageGRID. Usar certificados assinados (`-is-certificate-validation-enabled true`) de uma autoridade de certificação de terceiros é uma prática recomendada.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Exiba e verifique as informações de configuração do StorageGRID usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as informações de configuração do StorageGRID para o FabricPool.

Configure o ONTAP S3 como a camada de nuvem da ONTAP FabricPool

Se você estiver executando o ONTAP 9.8 ou posterior, poderá configurar o ONTAP S3 como a camada de nuvem do FabricPool.

O que você vai precisar

Você deve ter o nome do servidor ONTAP S3 e o endereço IP de seus LIFs associados no cluster remoto.

> O nome do servidor é usado como o nome de domínio totalmente qualificado (FQDN) por aplicativos cliente. Fora do ONTAP, confirme que os Registros DNS apontam para as LIFs de dados da SVM que estão sendo usadas.

Deve haver LIFs entre clusters no cluster local.

"Criação de LIFs entre clusters para disposição remota de FabricPool em camadas"

Sobre esta tarefa

O balanceamento de carga está habilitado para servidores ONTAP S3 no ONTAP 9.8 e posterior. Quando o nome do host do servidor resolve mais de um endereço IP, o ONTAP estabelece conexões de cliente com todos os endereços IP retornados (até um máximo de 16 endereços IP). Os endereços IP são coletados em um método round-robin quando as conexões são estabelecidas.

Procedimentos

Você pode configurar o ONTAP S3 como a categoria de nuvem para o FabricPool com o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

System Manager

1. Clique em **armazenamento > camadas > Adicionar nível de nuvem** e selecione ONTAP S3 como o provedor de armazenamento de objetos.
2. Preencha as informações solicitadas.
3. Se você quiser criar um espelho na nuvem, clique em **Adicionar como espelho FabricPool**.

Um espelhamento do FabricPool fornece um método para você substituir perfeitamente um armazenamento de dados e ajuda a garantir que seus dados estejam disponíveis em caso de desastre.

CLI

1. Adicione entradas para o servidor S3 e LIFs ao servidor DNS.

Opção	Descrição
Se você usar um servidor DNS externo	Atribua o nome do servidor S3 e os endereços IP ao administrador do servidor DNS.
Se você usar a tabela hosts DNS do sistema local	Introduza o seguinte comando: `dns host create -vserver svm_name -address ip_address -hostname s3_server_name`

2. Especifique as informações de configuração do ONTAP S3 usando o `storage aggregate object-store config create` comando com o `-provider-type ONTAP_S3` parâmetro.
   - O `storage aggregate object-store config create` comando falhará se o sistema ONTAP local não puder acessar o servidor ONTAP S3 com as informações fornecidas.
   - Use o `-access-key` parâmetro para especificar a chave de acesso para autorizar solicitações ao servidor ONTAP S3.
   - Use o `-secret-password` parâmetro para especificar a senha (chave de acesso secreto) para autenticar solicitações para o servidor ONTAP S3.
   - Se a senha do servidor ONTAP S3 for alterada, você deverá atualizar imediatamente a senha correspondente armazenada no sistema ONTAP local.

     Isso permite o acesso aos dados no armazenamento de objetos do ONTAP S3 sem interrupção.
   - Definir o `-is-certificate-validation-enabled` parâmetro para `false` desativa a verificação de certificados para o ONTAP S3. Usar certificados assinados (`-is-certificate-validation-enabled true`) de uma autoridade de certificação de terceiros é uma prática recomendada.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Exiba e verifique as informações de configuração do ONTAP_S3 usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as `ONTAP_S3` informações de configuração do FabricPool.

Configurar o Alibaba Cloud Object Storage como a camada de nuvem do ONTAP FabricPool

Se você estiver executando o ONTAP 9.6 ou posterior, poderá configurar o Alibaba Cloud Object Storage como a camada de nuvem para FabricPool.

Considerações para usar o storage de objetos na nuvem Alibaba com FabricPool

- A "Licença de disposição em camadas do BlueXP" é necessário ao fazer categorias no Alibaba Cloud Object Storage.
- Nos sistemas AFF e FAS e ONTAP Select, o FabricPool oferece suporte às seguintes classes de serviço de storage de objetos Alibaba:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service Acesso não frequente

    "Alibaba Cloud: Introdução às classes de armazenamento"

Entre em Contato com o representante de vendas da NetApp para obter informações sobre classes de armazenamento não listadas.

Passos

1. Especifique as informações de configuração do Alibaba Cloud Object Storage usando o `storage aggregate object-store config create` comando com o `-provider-type AliCloud` parâmetro.

   - O `storage aggregate object-store config create` comando falhará se o ONTAP não puder acessar o Alibaba Cloud Object Storage com as informações fornecidas.
   - Use o `-access-key` parâmetro para especificar a chave de acesso para autorizar solicitações ao armazenamento de objetos Alibaba Cloud Object Storage.
   - Se a senha do Alibaba Cloud Object Storage for alterada, você deverá atualizar a senha correspondente armazenada no ONTAP imediatamente.

     Com isso, o ONTAP pode acessar os dados no Alibaba Cloud Object Storage sem interrupção.

   ```
   storage aggregate object-store config create my_ali_oss_store_1
   -provider-type AliCloud -server oss-us-east-1.aliyuncs.com
   -container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
   ```

2. Exiba e verifique as informações de configuração do Alibaba Cloud Object Storage usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as informações de configuração do Alibaba Cloud Object Storage para FabricPool.

Configure o Amazon S3 como a camada de nuvem do ONTAP FabricPool

Se você estiver executando o ONTAP 9.2 ou posterior, poderá configurar o Amazon S3 como a camada de nuvem para o FabricPool. Se você estiver executando o ONTAP 9.5 ou posterior, poderá configurar o Amazon Commercial Cloud Services (C2S) para FabricPool.

Considerações para usar o Amazon S3 com FabricPool

- A "Licença de disposição em camadas do BlueXP" é necessário ao fazer a disposição em categorias no Amazon S3.
- Recomenda-se que o LIF que o ONTAP usa para se conetar ao servidor de objetos Amazon S3 esteja em uma porta de 10 Gbps.
- Nos sistemas AFF e FAS e ONTAP Select, o FabricPool oferece suporte às seguintes classes de storage do Amazon S3:
  - Padrão Amazon S3
  - Amazon S3 Standard - Acesso não frequente (Standard - IA)
  - Amazon S3 One Zone - Acesso não frequente (uma zona - IA)
  - Disposição em camadas inteligente do Amazon S3
  - Amazon Commercial Cloud Services
  - A partir do ONTAP 9.11,1, recuperação instantânea do Amazon S3 Glacier (o FabricPool não suporta recuperação flexível do Glacier ou arquivamento profundo do Glacier)

    "Documentação do Amazon Web Services: Classes de armazenamento do Amazon S3"

  Entre em Contato com seu representante de vendas para obter informações sobre classes de armazenamento não listadas.

- No Cloud Volumes ONTAP, o FabricPool oferece suporte à disposição em camadas de volumes SSD de uso geral (GP2) e HDD (st1) otimizados para taxa de transferência do Amazon Elastic Block Store (EBS).

Passos

1. Especifique as informações de configuração do Amazon S3 usando o `storage aggregate object-store config create` comando com o `-provider-type AWS_S3` parâmetro.
   - Você usa o `-auth-type CAP` parâmetro para obter credenciais para o acesso C2S.

     Quando você usa o `-auth-type CAP` parâmetro, você deve usar o `-cap-url` parâmetro para especificar o URL completo para solicitar credenciais temporárias para acesso C2S.

   - O `storage aggregate object-store config create` comando falhará se o ONTAP não puder acessar o Amazon S3 com as informações fornecidas.
   - Use o `-access-key` parâmetro para especificar a chave de acesso para autorizar solicitações ao armazenamento de objetos do Amazon S3.
   - Use o `-secret-password` parâmetro para especificar a senha (chave de acesso secreto) para autenticar solicitações no armazenamento de objetos do Amazon S3.
   - Se a senha do Amazon S3 for alterada, você deverá atualizar a senha correspondente armazenada no ONTAP imediatamente.

Isso permite que o ONTAP acesse os dados no Amazon S3 sem interrupção.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. Exiba e verifique as informações de configuração do Amazon S3 usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as informações de configuração do Amazon S3 para o FabricPool.

Configure o Google Cloud Storage como a camada de nuvem do ONTAP FabricPool

Se você estiver executando o ONTAP 9.6 ou posterior, poderá configurar o Google Cloud Storage como a camada de nuvem do FabricPool.

Considerações adicionais sobre como usar o Google Cloud Storage com FabricPool

- É necessário usar a "Licença de disposição em camadas do BlueXP"disposição em categorias no Google Cloud Storage.
- Recomenda-se que o LIF que o ONTAP usa para se conetar ao servidor de objetos Google Cloud Storage esteja em uma porta de 10 Gbps.
- Nos sistemas AFF e FAS e ONTAP Select, o FabricPool é compatível com as seguintes classes de storage de objetos do Google:
  - Multi-regional do Google Cloud
  - Google Cloud Regional
  - Google Cloud Nearline
  - Google Cloud Coldline

  "Google Cloud: Classes de armazenamento"

Passos

1. Especifique as informações de configuração do Google Cloud Storage usando o `storage aggregate object-store config create` comando com o `-provider-type GoogleCloud` parâmetro.

   - O `storage aggregate object-store config create` comando falhará se o ONTAP não

puder acessar o Google Cloud Storage com as informações fornecidas.

- Use o `-access-key` parâmetro para especificar a chave de acesso para autorizar solicitações ao armazenamento de objetos do Google Cloud Storage.
- Se a senha do Google Cloud Storage for alterada, você deve atualizar a senha correspondente armazenada no ONTAP imediatamente.

  Com isso, o ONTAP pode acessar os dados no Google Cloud Storage sem interrupção.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud  -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Exiba e verifique as informações de configuração do Google Cloud Storage usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as informações de configuração do Google Cloud Storage para FabricPool.

Configure o IBM Cloud Object Storage como a camada de nuvem do ONTAP FabricPool

Se você estiver executando o ONTAP 9.5 ou posterior, poderá configurar o IBM Cloud Object Storage como a camada de nuvem do FabricPool.

Considerações sobre o uso do IBM Cloud Object Storage com FabricPool

- A "Licença de disposição em camadas do BlueXP"é necessário ao dispor em camadas no IBM Cloud Object Storage.
- Recomenda-se que o LIF que o ONTAP usa para se conetar ao servidor de objetos IBM Cloud esteja em uma porta de 10 Gbps.

Passos

1. Especifique as informações de configuração do IBM Cloud Object Storage usando o `storage aggregate object-store config create` comando com o `-provider-type IBM_COS` parâmetro.

   - O `storage aggregate object-store config create` comando falhará se o ONTAP não puder acessar o IBM Cloud Object Storage com as informações fornecidas.
   - Use o `-access-key` parâmetro para especificar a chave de acesso para autorizar solicitações ao armazenamento de objetos IBM Cloud Object Storage.
   - Use o `-secret-password` parâmetro para especificar a senha (chave de acesso secreto) para autenticar solicitações no armazenamento de objetos do IBM Cloud Object Storage.
   - Se a senha do IBM Cloud Object Storage for alterada, você deverá atualizar a senha correspondente armazenada no ONTAP imediatamente.

     Com isso, o ONTAP pode acessar os dados no IBM Cloud Object Storage sem interrupção.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Exiba e verifique as informações de configuração do IBM Cloud Object Storage usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as informações de configuração do IBM Cloud Object Storage para FabricPool.

Configurar o storage de Blobs do Azure como a categoria de nuvem do ONTAP FabricPool

Se você estiver executando o ONTAP 9,4 ou posterior, poderá configurar o armazenamento de Blobs do Azure como a categoria de nuvem do FabricPool.

Considerações sobre o uso do armazenamento de Blobs do Microsoft Azure com FabricPool

- A "Licença de disposição em camadas do BlueXP"é necessário ao dispor em categorias no armazenamento de Blob do Azure.
- Não é necessária uma licença do FabricPool se você estiver usando o armazenamento de Blobs do Azure com Cloud Volumes ONTAP.
- É recomendável que o LIF que o ONTAP usa para se conetar ao servidor de objetos armazenamento de Blobs do Azure esteja em uma porta de 10 Gbps.
- No momento, o FabricPool não oferece suporte ao Azure Stack, que é serviços do Azure no local.
- No nível da conta no armazenamento de Blobs do Microsoft Azure, o FabricPool é compatível apenas com camadas de storage ativas e frias.

  O FabricPool não é compatível com a disposição em camadas no nível do blob. Ele também não é compatível com a disposição em camadas na camada de storage de arquivamento do Azure.

Sobre esta tarefa

No momento, o FabricPool não oferece suporte ao Azure Stack, que é serviços do Azure no local.

Passos

1. Especifique as informações de configuração do armazenamento de Blobs do Azure usando o `storage aggregate object-store config create` comando com o `-provider-type Azure_Cloud` parâmetro.

   - O `storage aggregate object-store config create` comando falhará se o ONTAP não puder acessar o armazenamento de Blobs do Azure com as informações fornecidas.
   - Você usa o `-azure-account` parâmetro para especificar a conta de armazenamento de Blobs do Azure.
   - Use o `-azure-private-key` parâmetro para especificar a chave de acesso para autenticar solicitações para armazenamento de Blobs do Azure.
   - Se a senha de armazenamento de Blobs do Azure for alterada, você deve atualizar a senha correspondente armazenada no ONTAP imediatamente.

Com isso, o ONTAP pode acessar os dados no armazenamento de Blobs do Azure sem interrupção.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Exiba e verifique as informações de configuração do armazenamento de Blobs do Azure usando o `storage aggregate object-store config show` comando.

   O `storage aggregate object-store config modify` comando permite modificar as informações de configuração do armazenamento de Blobs do Azure para o FabricPool.

Configurar armazenamentos de objetos para FabricPool em uma configuração MetroCluster

Se você estiver executando o ONTAP 9.7 ou posterior, poderá configurar um FabricPool espelhado em uma configuração do MetroCluster para categorizar dados inativos em armazenamentos de objetos em duas zonas de falha diferentes.

Sobre esta tarefa

- O FabricPool no MetroCluster exige que o agregado espelhado subjacente e a configuração de armazenamento de objetos associada sejam de propriedade da mesma configuração do MetroCluster.
- Não é possível anexar um agregado a um armazenamento de objetos criado no site MetroCluster remoto.
- Você deve criar configurações de armazenamento de objetos na configuração do MetroCluster que possua o agregado.

Antes de começar

- A configuração do MetroCluster está configurada e configurada corretamente.
- Dois armazenamentos de objetos são configurados nos sites MetroCluster apropriados.
- Os contentores são configurados em cada um dos armazenamentos de objetos.
- Os espaços IP são criados ou identificados nas duas configurações do MetroCluster e seus nomes coincidem.

Passo

1. Especifique as informações de configuração do armazenamento de objetos em cada site do MetroCluster usando o `storage object-store config create` comando.

   Neste exemplo, o FabricPool é necessário em apenas um cluster na configuração do MetroCluster. Duas configurações de armazenamento de objetos são criadas para esse cluster, uma para cada bucket do armazenamento de objetos.

```
storage aggregate
    object-store config create -object-store-name mcc1-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
    -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
<true|false> -provider <provider-type>
    -is-ssl-enabled <true|false> ipspace <IPSpace>
```

Este exemplo configura o FabricPool no segundo cluster na configuração do MetroCluster.

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

Testar a latência e a performance da taxa de transferência da camada de nuvem do ONTAP

Antes de anexar um armazenamento de objetos a um nível local, você pode testar a latência e o desempenho da taxa de transferência do armazenamento de objetos usando o profiler de armazenamento de objetos.

Antes de você ser

- É necessário adicionar a camada de nuvem ao ONTAP antes de usá-la com o profiler de armazenamento de objetos.
- Você deve estar no modo de privilégio avançado da CLI do ONTAP.

Passos

1. Inicie o profiler de armazenamento de objetos:

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. Veja os resultados:

   ```
   storage aggregate object-store profiler show
   ```

Associar a camada de nuvem do ONTAP a um nível local (agregado)

Depois de configurar um armazenamento de objetos como o nível de nuvem, especifique o nível local (agregado) a ser usado anexando-o ao FabricPool. No ONTAP 9.5 e posterior, você também pode anexar camadas locais (agregados) que contêm componentes de volume FlexGroup qualificados.

Sobre esta tarefa

Conectar uma camada de nuvem a um nível local é uma ação permanente. Um nível de nuvem não pode ser desanexado de um nível local depois de ser anexado. No entanto, você pode usar "Espelho FabricPool" para anexar um nível local a um nível de nuvem diferente.

Antes de começar

Quando você usa a CLI do ONTAP para configurar um agregado para o FabricPool, o agregado já deve existir.

> Quando você usa o Gerenciador de sistema para configurar um nível local para o FabricPool, você pode criar o nível local e configurá-lo para uso no FabricPool ao mesmo tempo.

Passos

É possível anexar um nível local (agregado) a um armazenamento de objetos do FabricPool com o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

System Manager

1. Navegue até **Storage > Tiers**, selecione um nível de nuvem e clique em .
2. Selecione **Anexar níveis locais**.
3. Em **Adicionar como primário**, verifique se os volumes estão qualificados para anexar.
4. Se necessário, selecione **Converter volumes para thin Provisioning**.
5. Clique em **Salvar**.

CLI

Para anexar um armazenamento de objetos a um agregado com a CLI:

1. **Opcional**: Para ver quantos dados em um volume estão inativos, siga as etapas em "Determinar a quantidade de dados em um volume estão inativos usando relatórios de dados inativos".

   Ver quantos dados em um volume estão inativos pode ajudá-lo a decidir qual agregado usar para o FabricPool.

2. Anexe o armazenamento de objetos a um agregado usando o `storage aggregate object-store attach` comando.

   Se o agregado nunca tiver sido usado com o FabricPool e contiver volumes existentes, a política de disposição em camadas padrão será atribuída aos volumes `snapshot-only`.

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

   Você pode usar a `allow-flexgroup true` opção para anexar agregados que contêm componentes de volume FlexGroup.

3. Exiba as informações do armazenamento de objetos e verifique se o armazenamento de objetos anexado está disponível usando o `storage aggregate object-store show` comando.

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   myaggr       Amazon01B1           available
   ```

Coloque os dados em categorias no bucket local

A partir do ONTAP 9.8, você pode categorizar dados no storage de objetos local usando o ONTAP S3.

A disposição em categorias dos dados em um bucket local é uma alternativa simples à migração dos dados para uma categoria local diferente. Esse procedimento usa um bucket existente no cluster local ou permite que o ONTAP crie automaticamente uma nova VM de storage e um novo bucket.

Lembre-se que depois de conectar a um nível local (agregado), a categoria de nuvem não pode ser desvinculada.

Uma licença S3 é necessária para esse fluxo de trabalho, que cria um novo servidor S3 e um novo bucket, ou usa os existentes. Esta licença incluída no "ONTAP One". Não é necessária uma licença FabricPool para este fluxo de trabalho.

Passo

1. Categorize os dados em um intervalo local: Clique em **níveis**, selecione um nível e clique em .
2. Se necessário, ative o thin Provisioning.
3. Escolha um nível existente ou crie um novo.
4. Se necessário, edite a política de disposição em camadas existente.

Gerenciar o FabricPool

Analise dados inativos do ONTAP com relatórios de dados inativos

Ao ver a quantidade de dados em um volume inativos, você aproveita as camadas de storage. As informações nos relatórios de dados inativos ajudam você a decidir qual agregado usar para o FabricPool, se deseja mover um volume para dentro ou para fora do FabricPool ou se deseja modificar a política de disposição em camadas de um volume.

O que você vai precisar

Você deve estar executando o ONTAP 9.4 ou posterior para usar a funcionalidade de relatórios de dados inativos.

Sobre esta tarefa

- Relatórios de dados inativos não são suportados em alguns agregados.

  Não é possível ativar o relatório de dados inativos quando o FabricPool não pode ser ativado, incluindo as seguintes instâncias:

  - Agregados de raiz
  - MetroCluster agrega executando versões do ONTAP anteriores a 9,7
  - Flash Pool (agregados híbridos ou agregados SnapLock)
- O relatório de dados inativos é ativado por padrão em agregados em que qualquer volume tem compactação adaptável ativada.
- O relatório de dados inativos é ativado por padrão em todos os agregados SSD no ONTAP 9.6.
- O relatório de dados inativos é ativado por padrão no FabricPool Aggregate no ONTAP 9.4 e no ONTAP 9.5.
- Você pode habilitar a geração de relatórios de dados inativos em agregados que não sejam FabricPool usando a CLI do ONTAP, incluindo agregados de HDD, começando com ONTAP 9.6.

Procedimento

Você pode determinar a quantidade de dados inativos com o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

System Manager

1. Escolha uma das seguintes opções:
   - Quando houver agregados de HDD existentes, navegue até **Storage > Tiers** e clique ⋮ em for the Aggregate on which you want to enable inactive data reporting.
   - Quando nenhuma camada de nuvem estiver configurada, navegue até **Dashboard** e clique no link **Enable Inactive data reporting** (Ativar relatório de dados inativos) em **Capacity** (capacidade).

CLI

Para ativar relatórios de dados inativos com a CLI:

1. Se o agregado para o qual você deseja ver o relatório de dados inativos não for usado no FabricPool, ative o relatório de dados inativos para o agregado usando o `storage aggregate modify` comando com o `-is-inactive-data-reporting-enabled true` parâmetro.

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

   Você precisa ativar explicitamente a funcionalidade de relatórios de dados inativos em um agregado que não é usado para o FabricPool.

   Você não pode e não precisa ativar o relatório de dados inativos em um agregado habilitado para FabricPool porque o agregado já vem com relatórios de dados inativos. O `-is-inactive-data-reporting-enabled` parâmetro não funciona em agregados habilitados para FabricPool.

   O `-fields is-inactive-data-reporting-enabled` parâmetro `storage aggregate show` do comando mostra se o relatório de dados inativos está ativado em um agregado.

2. Para exibir a quantidade de dados inativos em um volume, use o `volume show` comando com o `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parâmetro.

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
------- ------ ----------------------------------
-----------------------------------------
vsim1   vol0   0B                                 0%
vs1     vs1rv1 0B                                 0%
vs1     vv1    10.34MB                            0%
vs1     vv2    10.38MB                            0%
4 entries were displayed.
```

   - O `performance-tier-inactive-user-data` campo exibe a quantidade de dados do usuário armazenados no agregado que estão inativos.

- O `performance-tier-inactive-user-data-percent` campo exibe qual porcentagem dos dados estão inativos no sistema de arquivos ativo e nas cópias Snapshot.
- Para um agregado que não é usado para o FabricPool, os relatórios de dados inativos usam a política de disposição em categorias para decidir a quantidade de dados que devem ser reportados como inativos.
  - Na `none` política de disposição em categorias, são usados 31 dias.
  - Para os `snapshot-only` e `auto`, os relatórios de dados inativos `tiering-minimum-cooling-days` usam o .
  - Para a `ALL` política, o relatório de dados inativos assume que os dados serão categorizados em um dia.

    Até que o período seja atingido, a saída indica "»-" para a quantidade de dados inativos em vez de um valor.
- Em um volume que faz parte do FabricPool, o que o ONTAP relata como inativo depende da política de disposição em camadas definida em um volume.
  - Na `none` política de disposição em categorias, o ONTAP informa a quantidade total de volume inativo por pelo menos 31 dias. Não é possível usar o `-tiering-minimum-cooling-days` parâmetro com a `none` política de disposição em camadas.
  - Para as `ALL` políticas de disposição em camadas , `snapshot-only` e `auto` , os relatórios de dados inativos não são suportados.

Gerenciar volumes para FabricPool

Crie um volume em um agregado ONTAP habilitado para FabricPool

Você pode adicionar volumes ao FabricPool criando novos volumes diretamente no agregado habilitado para FabricPool ou movendo volumes existentes de outro agregado para o agregado habilitado para FabricPool.

Ao criar um volume para o FabricPool, você tem a opção de especificar uma política de disposição em camadas. Se nenhuma política de disposição em camadas for especificada, o volume criado usará a política de disposição em camadas padrão `snapshot-only`. Para um volume com a `snapshot-only` política de disposição em camadas ou `auto` , você também pode especificar o período mínimo de resfriamento em camadas.

O que você vai precisar

- Definir um volume para usar a `auto` política de disposição em camadas ou especificar o período mínimo de resfriamento em camadas requer o ONTAP 9.4 ou posterior.
- O uso do FlexGroup volumes requer o ONTAP 9.5 ou posterior.
- A configuração de um volume para usar a `all` política de disposição em camadas requer o ONTAP 9.6 ou posterior.
- Definir um volume para usar o `-cloud-retrieval-policy` parâmetro requer ONTAP 9.8 ou posterior.

Passos

1. Crie um novo volume para o FabricPool usando o `volume create` comando.

- O `-tiering-policy` parâmetro opcional permite especificar a política de disposição em camadas para o volume.

  Você pode especificar uma das seguintes políticas de disposição em categorias:

  - `snapshot-only` (predefinição)
  - `auto`
  - `all`
  - `backup` (obsoleto)
  - `none`

    "Tipos de políticas de disposição em camadas do FabricPool"

- O `-cloud-retrieval-policy` parâmetro opcional permite que os administradores de cluster com nível de privilégio avançado substituam o comportamento padrão de migração ou recuperação da nuvem controlado pela política de disposição em camadas.

  Você pode especificar uma das seguintes políticas de recuperação de nuvem:

  - `default`

    A política de disposição em camadas determina quais dados são retirados, portanto, não há alteração na recuperação de dados na nuvem com `default` a política de recuperação de nuvem. Isso significa que o comportamento é o mesmo que nos lançamentos pré-ONTAP 9.8:

    - Se a política de disposição em camadas for `none` ou `snapshot-only`, então "deffect" significa que qualquer leitura de dados orientada pelo cliente é puxada da camada de nuvem para a camada de desempenho.
    - Se a política de disposição em camadas for `auto`, qualquer leitura aleatória orientada pelo cliente será puxada, mas não leituras sequenciais.
    - Se a política de disposição em camadas não for usada `all`, os dados orientados pelo cliente serão extraídos da camada de nuvem.

  - `on-read`

    Todas as leituras de dados orientadas pelo cliente são extraídas da camada de nuvem para a camada de performance.

  - `never`

    Nenhum dado orientado pelo cliente é extraído da camada de nuvem para a camada de performance

  - `promote`

    - Na política de disposição em categorias `none` , todos os dados de nuvem são extraídos da camada de nuvem para a categoria de performance
    - Para a política de disposição em camadas `snapshot-only` , todos os dados do sistema de arquivos ativo são extraídos da camada de nuvem para a camada de desempenho.

- O `-tiering-minimum-cooling-days` parâmetro opcional no nível de privilégio avançado permite

especificar o período mínimo de resfriamento de disposição em camadas para um volume que usa a `snapshot-only` política de disposição em camadas ou `auto` .

A partir do ONTAP 9.8, é possível especificar um valor entre 2 e 183 para os dias mínimos de resfriamento em categorias. Se você estiver usando uma versão do ONTAP anterior a 9,8, poderá especificar um valor entre 2 e 63 para os dias mínimos de resfriamento em categorias.

Exemplo de criação de um volume para o FabricPool

O exemplo a seguir cria um volume chamado "yvol1" no agregado habilitado para FabricPool "myFabricPool". A política de disposição em categorias está definida como `auto` e o período de resfriamento mínimo de disposição em categorias é definido como 45 dias:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

Informações relacionadas

"Gerenciamento de volumes do FlexGroup"

Mover um volume para um agregado ONTAP habilitado para FabricPool

Quando você move um volume para o FabricPool, você tem a opção de especificar ou alterar a política de disposição em camadas do volume com a movimentação. A partir do ONTAP 9.8, quando você move um volume não FabricPool com relatórios de dados inativos ativados, o FabricPool usa um mapa de calor para ler blocos direcionáveis e move dados inativos para a camada de capacidade no destino do FabricPool.

O que você vai precisar

Você deve entender como mudar a política de disposição em camadas pode afetar o tempo necessário para que os dados fiquem inativos e sejam movidos para a categoria de nuvem.

"O que acontece com a política de disposição em camadas quando você move um volume"

Sobre esta tarefa

Se um volume que não é FabricPool tiver a geração de relatórios de dados inativos ativada, quando você move um volume com política de disposição em categorias `auto` ou `snapshot-only` para um FabricPool, o FabricPool lê os blocos direcionáveis de temperatura de um arquivo de mapa de calor e usa essa temperatura para mover os dados inativos diretamente para a camada de capacidade no destino do FabricPool.

Você não deve usar a `-tiering-policy` opção na movimentação de volume se estiver usando o ONTAP 9.8 e quiser que o FabricPools use informações de relatórios de dados inativos para mover dados diretamente para o nível de capacidade. O uso dessa opção faz com que o FabricPools ignore os dados de temperatura e, em vez disso, siga o comportamento de movimentação de Releases antes do ONTAP 9.8.

Passo

1. Use o `volume move start` comando para mover um volume para o FabricPool.

   O `-tiering-policy` parâmetro opcional permite especificar a política de disposição em camadas para o volume.

   Você pode especificar uma das seguintes políticas de disposição em categorias:

- `snapshot-only` (predefinição)
- `auto`
- `all`
- `none` E "Tipos de políticas de disposição em camadas do FabricPool"

Exemplo de mover um volume para o FabricPool

O exemplo a seguir move um volume chamado "yvol2" do SVM "VS1" para o agregado habilitado para FabricPool "dest_FabricPool". O volume está explicitamente definido para usar a `none` política de disposição em camadas:

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool -tiering-policy none
```

Habilite o ONTAP volumes no FabricPool a gravar diretamente na nuvem

A partir do ONTAP 9.14,1, você pode ativar e desativar a gravação diretamente na nuvem em um volume novo ou existente em um FabricPool para permitir que os clientes NFS gravem dados diretamente na nuvem sem esperar pela disposição em camadas de varreduras. Os clientes SMB ainda gravam no nível de performance em um volume habilitado para gravação na nuvem. O modo de gravação em nuvem está desativado por padrão.

Ter a capacidade de gravar diretamente na nuvem é útil para casos como migrações, por exemplo, em que grandes quantidades de dados são transferidos para um cluster do que o cluster pode dar suporte na camada local. Sem o modo de gravação na nuvem, durante a migração, quantidades menores de dados são transferidas, depois categorizadas, transferidas e categorizadas novamente, até que a migração seja concluída. Com o modo de gravação na nuvem, esse tipo de gerenciamento não é mais necessário porque os dados nunca são transferidos para a camada local.

Antes de começar

- Você deve ser um administrador de cluster ou SVM.
- Você deve estar no nível de privilégio avançado.
- O volume deve ser um volume do tipo leitura-gravação.
- O volume precisa ter a política de disposição em categorias.

Habilite a gravação diretamente na nuvem durante a criação de volume

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Crie um volume e ative o modo de gravação na nuvem:

```
volume create -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled <true|false> -aggregate <local tier name>
```

O exemplo a seguir cria um volume chamado vol1 com gravação em nuvem habilitada no nível local do FabricPool (aggr1):

```
volume create -vserver vs1 -volume vol1 -is-cloud-write-enabled true
-aggregate aggr1
```

Habilite a gravação diretamente na nuvem em um volume existente

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Modificar um volume para ativar o modo de gravação na nuvem:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled true
```

O exemplo a seguir modifica o volume chamado vol1 para ativar a gravação na nuvem:

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled true
```

Desative a gravação diretamente na nuvem em um volume

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Desativar o modo de gravação em nuvem em um volume:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled false
```

O exemplo a seguir desativa o modo de gravação em nuvem no volume chamado vol1:

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled false
```

Ative os volumes ONTAP no FabricPool para executar heads de leitura agressivos

A partir do ONTAP 9.14,1, você pode ativar e desativar o modo agressivo de leitura antecipada em volumes no FabricPools. O modo de leitura antecipada agressivo está disponível no ONTAP 9.14,1 em todas as plataformas locais compatíveis com FabricPool. O recurso está desativado por padrão.

Quando a leitura agressiva é *desabilitada*, o FabricPool só lê os blocos de arquivo que um aplicativo cliente precisa; ele não precisa ler o arquivo inteiro. Isso pode resultar em tráfego de rede reduzido, especialmente para grandes arquivos de tamanho GB e TB. *Habilitando* leitura antecipada agressiva em um volume desativa essa funcionalidade e o FabricPool lê preventivamente todo o arquivo sequencialmente do armazenamento de objetos, aumentando A taxa de transferência DE OBTENÇÃO e reduzindo a latência das leituras do cliente no arquivo. Por padrão, quando os dados em camadas são lidos sequencialmente, eles permanecem frios e não são gravados no nível local.

Eficiência de rede agressiva de leitura antecipada negoceia eficiência de rede para um melhor desempenho de dados em camadas.

Sobre esta tarefa

O `aggressive-readahead-mode` comando tem duas opções:

- `none`: a leitura antecipada está desativada.
- `file_prefetch`: o sistema lê o arquivo inteiro na memória antes do aplicativo cliente.

Antes de começar

- Você deve ser um administrador de cluster ou SVM.
- Você deve estar no nível de privilégio avançado.

Ative o modo de leitura antecipada agressivo durante a criação de volume

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Crie um volume e ative o modo de leitura antecipada agressivo:

```
volume create -volume <volume name>  -aggressive-readahead-mode
<none|file_prefetch>
```

O exemplo a seguir cria um volume chamado vol1 com leitura agressiva ativada com a opção file_prefetch:

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

Desativar o modo de leitura antecipada agressivo

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Desativar o modo de leitura antecipada agressivo:

```
volume modify -volume <volume name>  -aggressive-readahead-mode none
```

O exemplo a seguir modifica um volume chamado vol1 para desativar o modo agressivo de leitura antecipada:

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

Visualize o modo de leitura antecipada agressivo num volume

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Veja o modo agressivo de leitura antecipada:

```
volume show -fields aggressive-readahead-mode
```

Gerencie volumes ONTAP FabricPool com tags personalizadas criadas pelo usuário

A partir do ONTAP 9.8, o FabricPool oferece suporte à marcação de objetos usando tags personalizadas criadas pelo usuário para permitir classificar e classificar objetos para facilitar o gerenciamento. Se você for um usuário com o nível de privilégio de administrador, poderá criar novas tags de objeto e modificar, excluir e exibir tags existentes.

Atribua uma nova tag durante a criação de volume

Você pode criar uma nova tag de objeto quando quiser atribuir uma ou mais tags a novos objetos dispostos em camadas a partir de um novo volume criado. Você pode usar tags para ajudar a classificar e classificar

objetos em categorias para facilitar o gerenciamento de dados. A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para criar tags de objeto.

Sobre esta tarefa

Você pode definir tags apenas em volumes FabricPool anexados ao StorageGRID. Essas tags são mantidas durante uma movimentação de volume.

- É permitido um máximo de 4 etiquetas por volume.
- Na CLI, cada tag de objeto deve ser um par de chave-valor separado por um sinal igual.
- Na CLI, várias tags devem ser separadas por uma vírgula.
- Cada valor de tag pode conter um máximo de 127 carateres.
- Cada tecla de tag deve começar com um caractere alfabético ou um sublinhado.

  As teclas devem conter apenas carateres alfanuméricos e sublinhados, e o número máximo de carateres permitido é 127.

Você pode atribuir tags de objeto com o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

Exemplo 6. Passos

System Manager

1. Navegue até **Storage > Tiers**.
2. Localize uma camada de storage com volumes que você deseja etiquetar.
3. Clique na guia **volumes**.
4. Localize o volume que você deseja marcar e na coluna **Tags de objeto** selecione **clique para inserir tags**.
5. Introduza uma chave e um valor.
6. Clique em **aplicar**.

CLI

1. Use o `volume create` comando com a `-tiering-object-tags` opção para criar um novo volume com as tags especificadas. Você pode especificar várias tags em pares separados por vírgulas:

   ```
   volume create [ -vserver <vserver name> ] -volume <volume_name>
   -tiering-object-tags <key1=value1>
   [,<key2=value2>,<key3=value3>,<key4=value4> ]
   ```

   O exemplo a seguir cria um volume chamado fp_volume1 com três tags de objeto.

   ```
   vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
   project=fabricpool,type=abc,content=data
   ```

Modificar uma etiqueta existente

Você pode alterar o nome de uma tag, substituir tags em objetos existentes no armazenamento de objetos ou adicionar uma tag diferente a novos objetos que você planeja adicionar mais tarde.

Exemplo 7. Passos

System Manager

1. Navegue até **Storage > Tiers**.
2. Localize uma camada de storage com volumes que contêm tags que você deseja modificar.
3. Clique na guia **volumes**.
4. Localize o volume com as tags que deseja modificar e, na coluna **Tags de objeto**, clique no nome da tag.
5. Modifique a tag.
6. Clique em **aplicar**.

CLI

1. Use o `volume modify` comando com a `-tiering-object-tags` opção para modificar uma tag existente.

   ```
   volume modify [ -vserver <vserver name> ] -volume <volume_name>
   -tiering-object-tags <key1=value1> [ ,<key2=value2>,
   <key3=value3>,<key4=value4> ]
   ```

   O exemplo a seguir altera o nome da tag existente

   ```
   vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
   project=fabricpool,type=xyz,content=data
   ```

Excluir uma tag

Você pode excluir tags de objeto quando não quiser mais defini-las em um volume ou em objetos no armazenamento de objetos.

Exemplo 8. Passos

System Manager

1. Navegue até **Storage > Tiers**.
2. Localize um nível de storage com volumes que contêm tags que você deseja excluir.
3. Clique na guia **volumes**.
4. Localize o volume com as tags que você deseja excluir e, na coluna **Tags de objeto**, clique no nome da tag.
5. Para excluir a tag, clique no ícone da lixeira.
6. Clique em **aplicar**.

CLI

1. Use o `volume modify` comando com a `-tiering-object-tags` opção seguida de um valor vazio (`""`) para excluir uma tag existente.

   O exemplo a seguir exclui as tags existentes no fp_volume1.

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

Exibir tags existentes em um volume

Você pode exibir as tags existentes em um volume para ver quais tags estão disponíveis antes de anexar novas tags à lista.

Passos

1. Use o `volume show` comando com a `tiering-object-tags` opção para exibir tags existentes em um volume.

   ```
   volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
   tiering-object-tags
   ```

Verifique o status da marcação de objetos em volumes FabricPool

Você pode verificar se a marcação está concluída em um ou mais volumes do FabricPool.

Passos

1. Use o `vol show` comando com a `-fields needs-object-retagging` opção para ver se a marcação está em andamento, se ela foi concluída ou se a marcação não está definida.

   ```
   vol show -fields needs-object-retagging  [ -instance | -volume <volume
   name>]
   ```

   É apresentado um dos seguintes valores:

- `true`: o scanner de marcação de objetos ainda não foi executado ou precisa ser executado novamente para esse volume
- `false`: o scanner de marcação de objetos concluiu a marcação para este volume
- `<->`: o scanner de marcação de objetos não se aplica a este volume. Isso acontece para volumes que não residem no FabricPools.

Monitorar a utilização de espaço de um agregado ONTAP habilitado para FabricPool

Você precisa saber a quantidade de dados armazenados nas categorias de performance e nuvem do FabricPool. Essas informações ajudam a determinar se você precisa alterar a política de disposição em camadas de um volume, aumentar o limite de uso licenciado da FabricPool ou aumentar o espaço de storage da categoria de nuvem.

Passos

1. Monitore a utilização de espaço para agregados habilitados para FabricPool usando um dos seguintes comandos para exibir as informações:

Se você quiser exibir…	Em seguida, use este comando:
O tamanho usado da camada de nuvem em um agregado	`storage aggregate show` com o `-instance` parâmetro
Detalhes da utilização de espaço dentro de um agregado, incluindo a capacidade referenciada do armazenamento de objetos	`storage aggregate show-space` com o `-instance` parâmetro
Utilização de espaço dos armazenamentos de objetos anexados aos agregados, incluindo quanto espaço de licença está sendo usado	`storage aggregate object-store show-space`
Uma lista de volumes em um agregado e as pegadas de seus dados e metadados	`volume show-footprint`

Além de usar os comandos de CLI, você pode usar o Active IQ Unified Manager (anteriormente conhecido como Gerenciador Unificado de OnCommand), junto com o FabricPool Advisor, que é compatível com clusters ONTAP 9.4 e posteriores, ou o System Manager para monitorar a utilização de espaço.

O exemplo a seguir mostra maneiras de exibir a utilização de espaço e informações relacionadas ao FabricPool:

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                      ...
                                                 Aggregate Display Name:
MyFabricPool
                                                                      ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                      ...
                                                          Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                    Total Logical Used
Size: -
                                                    Logical Used
Percentage: -
                                              Logical Unreferenced
Capacity: -
                                            Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
                           ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume : rootvol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Volume Guarantee                 MB          %
Flexible Volume Metadata         KB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %

Vserver : vs1
Volume : vol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Footprint in Performance Tier    KB          %
Footprint in Amazon01            KB          %
Flexible Volume Metadata         MB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %
...
```

2. Execute uma das seguintes ações, conforme necessário:

Se você quiser…	Então…
Alterar a política de disposição em camadas de um volume	Siga o procedimento descrito "Gerenciamento da disposição em camadas de storage modificando a política de disposição em camadas de um volume ou o período mínimo de resfriamento em camadas"em .
Aumente o limite de uso licenciado da FabricPool	Entre em Contato com seu NetApp ou representante de vendas do parceiro. "Suporte à NetApp"
Aumente o espaço de storage da camada de nuvem	Entre em Contato com o fornecedor do armazenamento de objetos que você usa para o nível de nuvem.

Modificar a política de disposição em camadas de um volume ONTAP e o período mínimo de resfriamento

Você pode alterar a política de disposição em categorias de um volume para controlar se os dados são movidos para a categoria de nuvem quando ficam inativos (*cold*). No caso de um volume com a `snapshot-only` política de disposição em camadas ou `auto` , você também pode especificar o período mínimo de resfriamento de disposição em camadas que os dados do usuário devem permanecer inativos antes de serem movidos para a categoria de nuvem.

O que você vai precisar

Alterar um volume para a `auto` política de disposição em camadas ou modificar o período mínimo de resfriamento em camadas requer o ONTAP 9.4 ou posterior.

Sobre esta tarefa

A alteração da política de disposição em camadas de um volume altera apenas o comportamento de disposição em camadas subsequente do volume. Ele não migra os dados para a camada de nuvem de forma retroativa.

Alterar a política de disposição em camadas pode afetar quanto tempo leva para os dados ficarem inativos e serem movidos para a camada de nuvem.

"O que acontece quando você modifica a política de disposição em camadas de um volume no FabricPool"

Passos

1. Modifique a política de disposição em camadas para um volume existente usando o `volume modify` comando com o `-tiering-policy` parâmetro:

   Você pode especificar uma das seguintes políticas de disposição em categorias:

   - `snapshot-only` (predefinição)
   - `auto`
   - `all`
   - `none`

     "Tipos de políticas de disposição em camadas do FabricPool"

2. Se o volume usar a `snapshot-only` política de disposição em camadas ou `auto` e você quiser modificar o período mínimo de resfriamento em camadas, use o `volume modify` comando com o `-tiering-minimum-cooling-days` parâmetro opcional no nível avançado de privilégio.

   Você pode especificar um valor entre 2 e 183 para os dias mínimos de resfriamento em categorias. Se você estiver usando uma versão do ONTAP anterior a 9,8, poderá especificar um valor entre 2 e 63 para os dias mínimos de resfriamento em categorias.

Exemplo de modificação da política de disposição em camadas e do período mínimo de resfriamento de um volume

O exemplo a seguir altera a política de disposição em camadas do volume "myvol" no SVM "'VS1" `auto` e o período mínimo de resfriamento em camadas para 45 dias:

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

Arquivar volumes com FabricPool (vídeo)

Este vídeo mostra uma visão geral rápida do uso do Gerenciador de sistema para arquivar um volume em uma camada de nuvem com o FabricPool.

"Vídeo NetApp: Arquivamento de volumes com FabricPool (backup e movimentação de volume)"

Informações relacionadas

"NetApp TechComm TV: Lista de reprodução do FabricPool"

Modificar a política de disposição em camadas padrão do FabricPool de um volume ONTAP

Você pode alterar a política de disposição em camadas padrão de um volume para controlar a recuperação de dados do usuário da camada de nuvem para a camada de performance usando a `-cloud-retrieval-policy` opção introduzida no ONTAP 9.8.

O que você vai precisar

- Modificar um volume usando a `-cloud-retrieval-policy` opção requer ONTAP 9.8 ou posterior.
- Tem de ter o nível de privilégio avançado para executar esta operação.
- Você deve entender o comportamento das políticas de disposição em camadas com `-cloud-retrieval-policy`o .

  "Como as políticas de disposição em camadas funcionam com a migração para a nuvem"

Passo

1. Modifique o comportamento da diretiva de disposição em camadas para um volume existente usando o `volume modify` comando com a `-cloud-retrieval-policy` opção:

```
 volume create -volume <volume_name> -vserver <vserver_name> - tiering-
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
promote
```

O acelerador FabricPool coloca

Como administrador de storage, você pode usar o CONTROLE DE COLOCAÇÃO para definir um limite superior na taxa de colocação máxima por nó.

A OTIMIZAÇÃO DE PUT é útil quando os recursos de rede ou o endpoint do armazenamento de objetos são limitados a recursos. Embora raras, restrições de recursos podem ocorrer com armazenamentos de objetos

com baixo consumo de energia ou durante os primeiros dias de uso do FabricPool, quando TB ou PB de dados inativos começam a ficar em camadas.

A regulagem DA COLOCAÇÃO é por nó. O limite mínimo DE PUT-rate-limit é de 8MBMB/s. Definir o put-rate-limit para um valor inferior a 8MB MB/s resultará em taxa de transferência de 8MB MB/s nesse nó. Vários nós, em categorias simultâneas, podem consumir mais largura de banda e potencialmente saturar um link de rede com capacidade extremamente limitada.

> As operações do FabricPool PUT não competem por recursos com outras aplicações. As operações do FabricPool PUT são colocadas automaticamente em uma prioridade menor ("intimidadas") por aplicativos clientes e outras cargas de trabalho do ONTAP, como o SnapMirror. O uso de regulagem DE COLOCAÇÃO `put-rate-limit` pode ser útil para reduzir o tráfego de rede associado à disposição em camadas do FabricPool, mas não tem relação com o tráfego de ONTAP simultâneo.

Antes de começar

É necessário um nível de privilégio avançado.

Passos

1. O FabricPool do acelerador COLOCA as operações usando a CLI do ONTAP:

```
storage aggregate object-store put-rate-limit modify -node <name>
-default <true|false> -putrate-bytes-limit <integer>[KB|MB|GB|TB|PB]
```

Eliminação e desfragmentação de objetos FabricPool

O FabricPool não exclui blocos de armazenamentos de objetos anexados. Em vez disso, o FabricPool exclui objetos após uma determinada porcentagem dos blocos no objeto não serem mais referenciados pelo ONTAP.

Por exemplo, há 1.024 4KB blocos em um objeto 4MB dispostos em camadas no Amazon S3. Desfragmentação e exclusão não ocorrem até que menos de 205 4KB blocos (20% de 1.024) estejam sendo referenciados pelo ONTAP. Quando blocos suficientes (1.024) têm zero referências, seus objetos 4MB originais são excluídos e um novo objeto é criado.

Você pode personalizar a porcentagem de limite de espaço não recuperado e configurá-la para diferentes níveis padrão para diferentes armazenamentos de objetos. As predefinições são:

Armazenamento de objetos	ONTAP 9 .3 e anteriores	ONTAP 9,4 a 9,7	ONTAP 9 F.8 e mais tarde	Cloud Volumes ONTAP
Amazon S3	0%	20%	20%	30%
Google Cloud Storage	n/a.	12%	20%	35%
Storage Blob do Microsoft Azure	n/a.	15%	25%	35%

NetApp ONTAP S3	n/a.	n/a.	40%	n/a.
NetApp StorageGRID	0%	40%	40%	n/a.

Limite de espaço não recuperado

Alterar as configurações padrão de limite de espaço não recuperado aumentará ou diminuirá a quantidade aceita de fragmentação de objetos. Reduzir a fragmentação reduzirá a quantidade de capacidade física usada pela camada de nuvem em detrimento de recursos adicionais de armazenamento de objetos (leituras e gravações).

Redução do limiar

Para evitar despesas adicionais, considere reduzir os limites de espaço não recuperado ao usar esquemas de preços de armazenamento de objetos que reduzem o custo de storage, mas aumentam o custo das leituras. Os exemplos incluem o Amazon's Standard-IA e o armazenamento Blob do Azure Cool.

Por exemplo, a disposição em camadas de um volume de projetos de 10 anos que tenha sido economizado por razões legais pode ser mais barata ao usar um esquema de preços como Standard-IA ou Cool do que seria ao usar esquemas de preços padrão. Embora as leituras sejam mais caras para esse volume, incluindo leituras exigidas pela desfragmentação de objetos, é improvável que ocorram com frequência.

O limite aumenta

Como alternativa, considere aumentar os limites de espaço não recuperado se a fragmentação de objeto causar significativamente mais capacidade de armazenamento de objetos a ser usada do que o necessário para os dados referenciados pelo ONTAP. Por exemplo, usar um limite de espaço não recuperado de 20% em um cenário pior, em que todos os objetos estão igualmente fragmentados na extensão máxima permitida significa que é possível que 80% da capacidade total na camada de nuvem não seja referenciada pelo ONTAP. Por exemplo:

O 2TB referenciado pelo ONTAP e o 8TB não referenciado pelo ONTAP representa a capacidade total de 10TB TB usada pela camada de nuvem.

Nessa situação, pode ser vantajoso aumentar o limite de espaço não recuperado ou aumentar o volume de dias mínimos de resfriamento para reduzir a capacidade usada por blocos não referenciados.

> À medida que os objetos são desfragmentados e tornam o armazenamento mais eficiente, os arquivos subjacentes podem se tornar mais fragmentados à medida que os blocos referenciados são gravados em objetos novos e mais eficientes. Por esse motivo, o aumento significativo do limite de espaço não recuperado resulta em objetos com maior eficiência de storage, mas possivelmente reduz o desempenho de leitura sequencial.

Altere o limite de espaço não recuperado

Você pode personalizar a porcentagem de limite de espaço não recuperado para diferentes armazenamentos de objetos.

Antes de começar

É necessário um nível de privilégio avançado.

Passos

1. Para alterar o limite de espaço não recuperado padrão, personalize e execute o seguinte comando:

```
storage aggregate object-store modify -aggregate <name> -object-store
-name <name> -unreclaimedspace-threshold <%> (0%-99%)
```

Promover dados do ONTAP para o nível de performance

A partir do ONTAP 9.8, se você for um administrador de cluster no nível avançado de privilégio, poderá promover proativamente os dados para o nível de desempenho a partir da camada de nuvem usando uma combinação do `tiering-policy` e da `cloud-retrieval-policy` configuração.

Sobre esta tarefa

Você pode fazer isso se quiser parar de usar o FabricPool em um volume ou se tiver uma `snapshot-only` política de disposição em categorias e quiser trazer de volta os dados da cópia Snapshot restaurados para o nível de performance.

Promover todos os dados de um volume FabricPool para o nível de performance

Você pode recuperar proativamente todos os dados em um volume FabricPool na categoria de nuvem e promovê-los para a categoria de performance.

Passos

1. Use o `volume modify` comando para definir `tiering-policy` como `none` e `cloud-retrieval-policy` como `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

Promova os dados do sistema de arquivos para o nível de performance

Você pode recuperar proativamente os dados do sistema de arquivos ativos de uma cópia Snapshot restaurada na categoria de nuvem e promovê-los para a categoria de performance.

Passos

1. Use o `volume modify` comando para definir `tiering-policy` como `snapshot-only` e `cloud-retrieval-policy` como `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

Verifique o status de uma promoção de nível de desempenho

Você pode verificar o status da promoção do nível de performance para determinar quando a operação está

concluída.

Passos

1. Use o comando volume `object-store` com a `tiering` opção para verificar o status da promoção do nível de desempenho.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                  Vserver: vs1
                                   Volume: v1
                                Node Name: node1
                              Volume DSID: 1023
                           Aggregate Name: a1
                                    State: ready
                      Previous Run Status: completed
                Aborted Exception Status: -
              Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                Scanner Percent Complete: -
                     Scanner Current VBN: -
                        Scanner Max VBNs: -
     Time Waiting Scan will be scheduled: -
                          Tiering Policy: snapshot-only
    Estimated Space Needed for Promotion: -
                       Time Scan Started: -
  Estimated Time Remaining for scan to complete: -
                    Cloud Retrieve Policy: promote
```

Acione a migração e a disposição em camadas agendadas

A partir do ONTAP 9.8, você pode acionar uma solicitação de digitalização em categorias a qualquer momento, quando preferir não esperar pela verificação de disposição em categorias padrão.

Passos

1. Use o `volume object-store` comando com a `trigger` opção de solicitar migração e disposição em camadas.

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

Gerenciar espelhos FabricPool

Saiba mais sobre espelhos ONTAP FabricPool

Para garantir que os dados estejam acessíveis em armazenamentos de dados em caso de desastre e para permitir a substituição de um armazenamento de dados, é possível configurar um espelhamento FabricPool adicionando um segundo armazenamento de dados para categorizar dados de maneira síncrona em dois armazenamentos de dados . Você pode adicionar um segundo armazenamento de dados a configurações novas ou existentes do FabricPool, monitorar o status do espelhamento, exibir detalhes do espelho do FabricPool, promover um espelho e remover um espelho. Você deve estar executando o ONTAP 9.7 ou posterior.

Crie um espelho ONTAP FabricPool

Para criar um espelho FabricPool, anexe dois armazenamentos de objetos a um único FabricPool. Você pode criar um espelho FabricPool anexando um segundo armazenamento de objetos a uma configuração do FabricPool de armazenamento de objetos único existente ou pode criar uma nova configuração do FabricPool de armazenamento de objetos único e, em seguida, anexar um segundo armazenamento de objetos a ele. Você também pode criar espelhos FabricPool nas configurações do MetroCluster.

O que você vai precisar

- Você já deve ter criado os dois armazenamentos de objetos usando o `storage aggregate object-store config` comando.
- Se você estiver criando espelhos do FabricPool em configurações do MetroCluster:
  - Você já deve ter configurado e configurado o MetroCluster
  - Você deve ter criado as configurações de armazenamento de objetos no cluster selecionado.

    Se você estiver criando espelhos do FabricPool em ambos os clusters em uma configuração do MetroCluster, você precisará criar configurações de armazenamento de objetos nos dois clusters.

  - Se você não estiver usando armazenamentos de objetos no local para configurações do MetroCluster, verifique se existe um dos seguintes cenários:
    - Os armazenamentos de objetos estão em diferentes zonas de disponibilidade
    - Os armazenamentos de objetos são configurados para manter cópias de objetos em várias zonas de disponibilidade

      "Configurando armazenamentos de objetos para FabricPool em uma configuração MetroCluster"

Sobre esta tarefa

O armazenamento de objetos usado para o espelho FabricPool deve ser diferente do armazenamento de objetos primário.

O procedimento para criar um espelho FabricPool é o mesmo para configurações MetroCluster e não MetroCluster.

Passos

1. Se você não estiver usando uma configuração FabricPool existente, crie uma nova anexando um armazenamento de objetos a um agregado usando o `storage aggregate object-store attach` comando.

   Este exemplo cria um novo FabricPool anexando um armazenamento de objetos a um agregado.

   ```
   cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
   my-store-1
   ```

2. Anexe um segundo armazenamento de objetos ao agregado usando o `storage aggregate object-store mirror` comando.

   Este exemplo anexa um segundo armazenamento de objetos a um agregado para criar um espelho FabricPool.

   ```
   cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
   my-store-2
   ```

Apresentar detalhes do espelho ONTAP FabricPool

Você pode exibir detalhes sobre um espelho FabricPool para ver quais armazenamentos de objetos estão na configuração e se o espelho de armazenamento de objetos está em sincronia com o armazenamento de objetos primário.

Passo

1. Exiba informações sobre um espelho FabricPool usando o `storage aggregate object-store show` comando.

   Este exemplo exibe os detalhes sobre os armazenamentos de objetos primário e espelhado em um espelho FabricPool.

   ```
   cluster1::> storage aggregate object-store show
   ```

   ```
   Aggregate      Object Store Name Availability    Mirror Type
   -------------- ----------------- -------------   ----------
   aggr1          my-store-1        available       primary
                  my-store-2        available       mirror
   ```

   Este exemplo exibe detalhes sobre o espelho FabricPool, incluindo se o espelho está degradado devido a uma operação ressincronizada.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-store-1        primary           -
               my-store-2        mirror          false
```

Promova um espelho ONTAP FabricPool

Você pode reatribuir o espelho de armazenamento de objetos como o armazenamento de objetos principal promovendo-o. Quando o espelho de armazenamento de objetos se torna o principal, o primário original se torna automaticamente o espelho.

O que você vai precisar

- O espelho FabricPool deve estar sincronizado
- O armazenamento de objetos deve estar operacional

Sobre esta tarefa

Você pode substituir o armazenamento de objetos original por um armazenamento de objetos de um provedor de nuvem diferente. Por exemplo, seu espelho original pode ser um armazenamento de objetos da AWS, mas você pode substituí-lo por um armazenamento de objetos do Azure.

Passos

1. Verifique se o espelho FabricPool está em sincronia usando o `storage aggregate object-store show-resync-status` comando. Se o espelho FabricPool estiver em sincronia, nenhuma entrada será exibida. Se o espelho não estiver em sincronia, aguarde até que a ressincronização seja concluída.

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

```
                                          Complete
     Aggregate    Primary       Mirror     Percentage
     ---------    -----------   ----------    ----------
     aggr1        my-store-1     my-store-2     40%
```

2. Promova um espelho de armazenamento de objetos usando o `storage aggregate object-store modify -aggregate` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-store-2 -mirror-type primary
```

Retire um espelho ONTAP FabricPool

Você pode remover um espelho FabricPool se não precisar mais replicar um armazenamento de objetos.

O que você vai precisar

O armazenamento de objetos primário deve estar operacional; caso contrário, o comando falha.

Passo

1. Remova um espelho de armazenamento de objetos em um FabricPool usando o `storage aggregate object-store unmirror -aggregate` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

Substitua um armazenamento de objetos existente por um espelho ONTAP FabricPool

Você pode usar a tecnologia FabricPool mirror para substituir um armazenamento de objetos por outro. O novo armazenamento de objetos não precisa usar o mesmo provedor de nuvem que o armazenamento de objetos original.

Sobre esta tarefa

Você pode substituir o armazenamento de objetos original por um armazenamento de objetos que usa um provedor de nuvem diferente. Por exemplo, seu armazenamento de objetos original pode usar a AWS como provedor de nuvem, mas você pode substituí-lo por um armazenamento de objetos que usa o Azure como provedor de nuvem e vice-versa. No entanto, o novo armazenamento de objetos deve manter o mesmo tamanho de objeto que o original.

Passos

1. Crie um espelho FabricPool adicionando um novo armazenamento de objetos a um FabricPool existente usando o `storage aggregate object-store mirror` comando.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. Monitore o status de ressincronização do espelho usando o `storage aggregate object-store show-resync-status` comando.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                                Complete
      Aggregate    Primary          Mirror      Percentage
      ---------    -----------      ----------  ----------
      aggr1        my-AWS-store     my-AZURE-store     40%
```

3. Verifique se o espelho está em sincronia usando o `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. Troque o armazenamento de objetos primário pelo armazenamento de objetos espelhados usando o `storage aggregate object-store modify` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. Exiba detalhes sobre o espelho FabricPool usando o `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

   Este exemplo exibe as informações sobre o espelho FabricPool, incluindo se o espelho está degradado (não em sincronia).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. Extrair o espelho FabricPool com o `storage aggregate object-store unmirror` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Verifique se o FabricPool está de volta em uma configuração de armazenamento de objetos único usando o `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

Substitua um espelho FabricPool em uma configuração ONTAP MetroCluster

Se um dos objetos armazenados em um espelho FabricPool for destruído ou ficar permanentemente indisponível em uma configuração MetroCluster, você poderá fazer com que o objeto armazene o espelho se ele ainda não for o espelho, remover o armazenamento de objetos danificado do espelho FabricPool e, em seguida, adicionar um novo espelho de armazenamento de objetos ao FabricPool.

Passos

1. Se o armazenamento de objetos danificado ainda não for o espelho, faça com que o objeto armazene o espelho com o `storage aggregate object-store modify` comando.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mcc1_ostore1 -mirror-type mirror
```

2. Remova o espelho de armazenamento de objetos do FabricPool usando o `storage aggregate object-store unmirror` comando.

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mcc1_ostore1
```

3. Você pode forçar a disposição em categorias a ser retomada no armazenamento de dados primário depois de remover o armazenamento de dados espelhados usando `storage aggregate object-store modify` a opção com . `-force-tiering-on-metrocluster true`

   A ausência de um espelho interfere com os requisitos de replicação de uma configuração do MetroCluster.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. Crie um armazenamento de objetos de substituição usando o `storage aggregate object-store config create` comando.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Adicione o espelho de armazenamento de objetos ao espelho FabricPool usando o `storage aggregate object-store mirror` comando.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Exiba as informações do armazenamento de objetos usando o `storage aggregate object-store show` comando.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary           -
               mcc1_ostore3-mc    mirror          true
```

7. Monitore o status de ressincronização do espelho usando o `storage aggregate object-store show-resync-status` comando.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                              Complete
     Aggregate    Primary        Mirror          Percentage
     ---------    -----------    ----------      ----------
     aggr1        mcc1_ostore1-mc mcc1_ostore3-mc   40%
```

Comandos para gerenciar recursos do FabricPool

Você usa os `storage aggregate object-store` comandos para gerenciar armazenamentos de objetos para o FabricPool. Você usa os `storage aggregate` comandos para gerenciar agregados para FabricPool. Use os `volume` comandos para gerenciar volumes para FabricPool.

Se você quiser…	Use este comando:
Defina a configuração de um armazenamento de objetos para que o ONTAP possa acessá-lo	`storage aggregate object-store config create`
Modificar atributos de configuração do armazenamento de objetos	`storage aggregate object-store config modify`
Renomeie uma configuração de armazenamento de objetos existente	`storage aggregate object-store config rename`
Exclua a configuração de um armazenamento de objetos	`storage aggregate object-store config delete`
Exibir uma lista de configurações de armazenamento de objetos	`storage aggregate object-store config show`
Anexe um segundo armazenamento de objetos a um FabricPool novo ou existente como um espelho	`storage aggregate object-store mirror` com o `-aggregate` parâmetro e `-name` no nível de privilégio admin
Remova um espelho de armazenamento de objetos de um espelho FabricPool existente	`storage aggregate object-store unmirror` com o `-aggregate` parâmetro e `-name` no nível de privilégio admin
Monitorar o status de ressincronização do espelho FabricPool	`storage aggregate object-store show-resync-status`
Apresentar detalhes do espelho FabricPool	`storage aggregate object-store show`
Promova um espelho de armazenamento de objetos para substituir um armazenamento de objetos primário em uma configuração de espelhamento FabricPool	`storage aggregate object-store modify` com o `-aggregate` parâmetro no nível de privilégio admin
Teste a latência e o desempenho de um armazenamento de objetos sem anexar o armazenamento de objetos a um agregado	`storage aggregate object-store profiler start` com o `-object-store-name` parâmetro e `-node` no nível de privilégio avançado
Monitore o status do profiler do armazenamento de objetos	`storage aggregate object-store profiler show` com o `-object-store-name` parâmetro e `-node` no nível de privilégio avançado
Abortar o profiler de armazenamento de objetos quando estiver em execução	`storage aggregate object-store profiler abort` com o `-object-store-name` parâmetro e `-node` no nível de privilégio avançado

Anexe um armazenamento de objetos a um agregado para usar o FabricPool	`storage aggregate object-store attach`
Anexe um armazenamento de objetos a um agregado que contenha um volume FlexGroup para usar o FabricPool	`storage aggregate object-store attach` com o. `allow-flexgroup true`
Exiba detalhes dos armazenamentos de objetos anexados a agregados habilitados para FabricPool	`storage aggregate object-store show`
Exibir o limite de preenchimento agregado usado pelo exame de disposição em camadas	`storage aggregate object-store show` com o `-fields tiering-fullness-threshold` parâmetro no nível de privilégio avançado
Exibir a utilização de espaço dos armazenamentos de objetos anexados a agregados habilitados para FabricPool	`storage aggregate object-store show-space`
Ative relatórios de dados inativos em um agregado que não é usado para o FabricPool	`storage aggregate modify` com o `-is -inactive-data-reporting-enabled true` parâmetro
Exibir se o relatório de dados inativos está ativado em um agregado	`storage aggregate show` com o `-fields is-inactive-data-reporting-enabled` parâmetro
Exiba informações sobre a quantidade de dados do usuário inativos dentro de um agregado	`storage aggregate show-space` com o `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parâmetro
Crie um volume para o FabricPool, incluindo especificar o seguinte: • A política de disposição em camadas • O período de resfriamento mínimo de disposição em camadas (para a `snapshot-only` política de disposição em camadas ou `auto` disposição em camadas)	`volume create` • Use o `-tiering-policy` parâmetro para especificar a política de disposição em camadas. • Você usa o `-tiering-minimum-cooling -days` parâmetro no nível de privilégio avançado para especificar o período mínimo de resfriamento em camadas.
Modifique um volume para FabricPool, incluindo a modificação do seguinte: • A política de disposição em camadas • O período de resfriamento mínimo de disposição em camadas (para a `snapshot-only` política de disposição em camadas ou `auto` disposição em camadas)	`volume modify` • Use o `-tiering-policy` parâmetro para especificar a política de disposição em camadas. • Você usa o `-tiering-minimum-cooling -days` parâmetro no nível de privilégio avançado para especificar o período mínimo de resfriamento em camadas.

Exibir informações do FabricPool relacionadas a um volume, incluindo o seguinte: • O período mínimo de resfriamento em camadas • Quantos dados do usuário estão inativos	`volume show` • Você usa o `-fields tiering-minimum-cooling-days` parâmetro no nível de privilégio avançado para exibir o período mínimo de resfriamento em camadas. • Você usa o `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parâmetro para exibir a quantidade de dados do usuário frios.
Mover um volume para dentro ou para fora do FabricPool	`volume move start` Você usa o `-tiering-policy` parâmetro opcional para especificar a política de disposição em camadas para o volume.
Modifique o limite para recuperar espaço não referenciado (o limite de desfragmentação) para FabricPool	`storage aggregate object-store modify` com o `-unreclaimed-space-threshold` parâmetro no nível de privilégio avançado
Modifique o limite para a porcentagem completa que o agregado se torna antes que a varredura de disposição em camadas comece a disposição em camadas de dados para FabricPool A FabricPool continua categorizando dados pouco acessados em uma categoria de nuvem até que a categoria local atinja 98% de capacidade.	`storage aggregate object-store modify` com o `-tiering-fullness-threshold` parâmetro no nível de privilégio avançado
Exiba o limite para recuperar espaço não referenciado para o FabricPool	`storage aggregate object-store show` ou `storage aggregate object-store show-space` comande com o `-unreclaimed-space-threshold` parâmetro no nível de privilégio avançado

Mobilidade de dados do SVM

Visão geral da mobilidade de dados do SVM

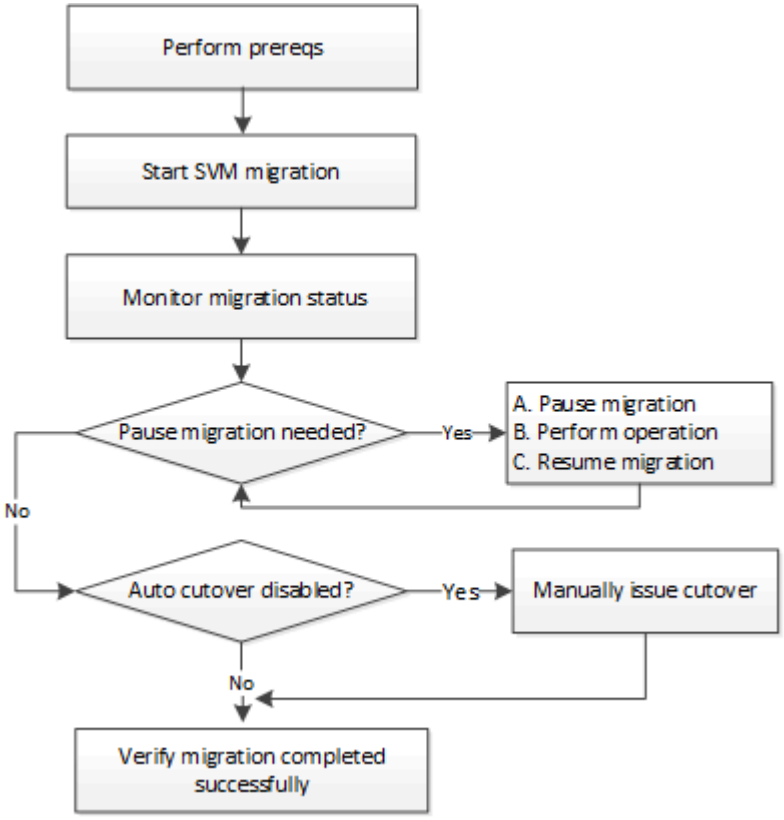
A partir do ONTAP 9.10,1, os administradores de cluster podem realocar um SVM de um cluster de origem para um cluster de destino para gerenciar a capacidade e o balanceamento de carga ou para habilitar upgrades de equipamentos ou consolidações de data center usando a CLI do ONTAP.

Essa funcionalidade de realocação contínua da SVM é compatível com plataformas AFF no ONTAP 9.10,1 e 9.11.1. A partir do ONTAP 9.12,1, essa funcionalidade é suportada nas plataformas FAS e AFF e em agregados híbridos.

O nome do SVM e UUID permanecem inalterados após a migração, bem como o nome do LIF de dados, endereço IP e nomes de objetos, como o nome do volume. A UUID dos objetos no SVM será diferente.

Fluxo de trabalho de migração da SVM

O diagrama mostra o fluxo de trabalho típico para uma migração SVM. Inicie uma migração para SVM a partir do cluster de destino. Pode monitorizar a migração a partir da origem ou do destino. Você pode fazer uma transferência manual ou uma transferência automática. Uma transição automática é realizada por padrão.



Compatibilidade com a plataforma de migração SVM

Família de controladores	Versões do ONTAP suportadas
AFF Série A.	ONTAP 9.10,1 e posterior
Série C AFF	ONTAP 9.12,1 patch 4 e posterior
FAS	ONTAP 9.12,1 e posterior

Ao migrar de um cluster AFF para um cluster FAS com agregados híbridos, o posicionamento automático de volume tentará executar uma correspondência de agregados semelhante a essa. Por exemplo, se o cluster de origem tiver 60 volumes, o posicionamento do volume tentará encontrar um agregado AFF no destino para colocar os volumes. Quando não houver espaço suficiente nos agregados AFF, os volumes serão colocados em agregados com discos não flash.

Suporte à escalabilidade pela versão ONTAP

Versão de ONTAP	Pares HA na origem e no destino

ONTAP 9.14,1	12
ONTAP 9.13,1	6
ONTAP 9.11,1	3
ONTAP 9.10,1	1

Requisitos de desempenho da infraestrutura de rede para o tempo de ida e volta (RTT) TCP entre a origem e o cluster de destino

Dependendo da versão do ONTAP instalada no cluster, a rede que coneta os clusters de origem e destino deve ter um tempo máximo de ida e volta, conforme indicado:

Versão de ONTAP	RTT máximo
ONTAP 9.12,1 e posterior	10ms
ONTAP 9.11,1 e anteriores	2ms

Máximo de volumes compatíveis por SVM

Fonte	Destino	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1 e anteriores
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	N/A.
FAS	AFF	80	80	80	N/A.
AFF	FAS	80	80	80	N/A.

Pré-requisitos

Antes de iniciar uma migração SVM, você deve atender aos seguintes pré-requisitos:

- Você deve ser um administrador de cluster.
- "Os clusters de origem e destino devem ser direcionados um para o outro".
- Os clusters de origem e destino devem ter o SnapMirror síncrono "licença instalada". Esta licença está incluída no "ONTAP One".
- Todos os nós no cluster de origem devem estar executando o ONTAP 9.10,1 ou posterior. Para obter suporte específico ao controlador de array ONTAP, "Hardware Universe"consulte .
- Todos os nós no cluster de origem devem estar executando a mesma versão do ONTAP.
- Todos os nós no cluster de destino devem estar executando a mesma versão do ONTAP.
- A versão do ONTAP do cluster de destino deve ser igual ou não mais do que duas versões mais recentes principais do cluster de origem.
- Os clusters de origem e destino devem suportar a mesma sub-rede IP para acesso a LIF de dados.
- O SVM de origem deve conter menos do que o número máximo de volumes de dados suportados para a versão.
- Espaço suficiente para a colocação do volume deve estar disponível no destino
- O Onboard Key Manager deve ser configurado no destino se o SVM de origem tiver volumes

criptografados

Prática recomendada

Ao executar uma migração para SVM, é uma prática recomendada deixar 30% de espaço livre de CPU no cluster de origem e no cluster de destino para permitir a execução do workload da CPU.

Operações da SVM

Você deve verificar se há operações que podem entrar em conflito com a migração da SVM:

- Nenhuma operação de failover está em andamento
- WAFLIRON não pode estar em funcionamento
- A impressão digital não está em andamento
- A movimentação de volume, o rehost, o clone, a criação, a conversão ou a análise não estão em execução

Recursos suportados e não suportados

A tabela indica os recursos do ONTAP compatíveis com mobilidade de dados do SVM e as versões do ONTAP em que o suporte está disponível.

Para obter informações sobre a interoperabilidade da versão do ONTAP entre uma origem e um destino em uma migração SVM, "Versões compatíveis do ONTAP para relacionamentos do SnapMirror"consulte .

Recurso	Lançamento primeiro suportado	Comentários
Proteção autônoma contra ransomware	ONTAP 9.12,1	
Cloud Volumes ONTAP	Não suportado	
Gerenciador de chaves externo	ONTAP 9.11,1	
FabricPool	ONTAP 9.11,1	A migração do SVM é compatível com volumes no FabricPools para as plataformas a seguir: • Plataforma Azure NetApp Files. Todas as políticas de disposição em categorias são compatíveis (somente snapshot, automático, all e nenhum).
Relação de fanout (a origem migrante tem um volume de origem SnapMirror com mais de um destino)	ONTAP 9.11,1	
FC SAN	Não suportado	
Flash Pool	ONTAP 9.12,1	

Volumes FlexCache	Não suportado	
FlexGroup	Não suportado	
Diretivas IPsec	Não suportado	
IPv6 LIFs	Não suportado	
San iSCSI	Não suportado	
Replicação do agendamento de trabalhos	ONTAP 9.11,1	No ONTAP 9.10,1, as programações de trabalhos não são replicadas durante a migração e devem ser criadas manualmente no destino. A partir do ONTAP 9.11,1, as programações de tarefas usadas pela origem são replicadas automaticamente durante a migração.
Espelhos de partilha de carga	Não suportado	
SVMs MetroCluster	ONTAP 9.16,1	É possível migrar um SVM de um par de HA que não seja MetroCluster para uma configuração MetroCluster ou de uma configuração MetroCluster para um par de HA que não seja MetroCluster. Não é possível migrar um SVM de uma configuração do MetroCluster para outra configuração do MetroCluster. [NOTA] a migração do SVM não é compatível com a migração do MetroCluster SVM em versões anteriores ao ONTAP 9.16,1. Talvez você possa usar a replicação assíncrona do SnapMirror para "Migrar um SVM em uma configuração do MetroCluster"o . Você deve estar ciente de que usar o SnapMirror assíncrono para migrar um SVM em uma configuração do MetroCluster é *disruptive* método de migração.
Criptografia de agregados NetApp (NAE)	Não suportado	A migração não é suportada para nenhum endpoint que utilize o NAE.
Configurações NDMP	Não suportado	
Criptografia de volume NetApp (NVE)	ONTAP 9.10,1	

Logs de auditoria NFS e SMB	ONTAP 9.13,1	Para a migração SVM no local com auditoria habilitada, você deve desativar a auditoria na SVM de origem e, em seguida, executar a migração. Antes da migração para o SVM: • "O redirecionamento do log de auditoria deve estar ativado no cluster de destino". • "O caminho de destino do log de auditoria da SVM de origem deve ser criado no cluster de destino".
NFS v3, NFS v4,1 e NFS v4,2	ONTAP 9.10,1	
NFS v4.0	ONTAP 9.12,1	
NFSv4,1 com pNFS	ONTAP 9.14,1	
NVMe sobre Fabric	Não suportado	
Gerenciador de chaves integrado (OKM) com o modo critérios comuns ativado no cluster de origem	Não suportado	
Qtrees	ONTAP 9.14,1	
Quotas	ONTAP 9.14,1	
S3	Não suportado	
Protocolo SMB	ONTAP 9.12,1	As migrações SMB são disruptivas e exigem uma atualização do cliente após a migração.
Relacionamentos de nuvem da SnapMirror	ONTAP 9.12,1	A partir do ONTAP 9.12,1, quando você migra um SVM no local com relacionamentos de nuvem do SnapMirror, o cluster de destino precisa ter o "Licença de nuvem da SnapMirror" instalado e ter capacidade suficiente disponível para dar suporte à migração de capacidade nos volumes espelhados para a nuvem.
Destino assíncrono SnapMirror	ONTAP 9.12,1	

Fonte assíncrona do SnapMirror	ONTAP 9.11,1	• As transferências podem continuar normalmente nas relações FlexVol SnapMirror durante a maior parte da migração. • Quaisquer transferências contínuas são canceladas durante a transição e novas transferências falham durante a transição e não podem ser reiniciadas até que a migração seja concluída. • As transferências agendadas que foram canceladas ou perdidas durante a migração não são iniciadas automaticamente após a conclusão da migração.  Quando uma fonte SnapMirror é migrada, o ONTAP não impede a exclusão do volume após a migração até que a atualização do SnapMirror ocorra. Isso acontece porque as informações relacionadas ao SnapMirror para volumes de origem SnapMirror migrados estão disponíveis somente após a conclusão da migração e após a primeira atualização.
Definições de SMTape	Não suportado	
SnapLock	Não suportado	
Sincronização ativa do SnapMirror	Não suportado	
Relacionamentos de pares SVM do SnapMirror	ONTAP 9.12,1	
Recuperação de desastres do SnapMirror SVM	Não suportado	
SnapMirror síncrono	Não suportado	
Instantâneos	ONTAP 9.10,1	
Bloqueio de snapshot à prova de violações	ONTAP 9.14,1	O bloqueio de snapshot à prova de violações não é equivalente ao SnapLock. O SnapLock Enterprise e o SnapLock Compliance permanecem sem suporte.
Virtual IP LIFs/BGP	Não suportado	

Console de armazenamento virtual 7,0 e posterior	Não suportado	
Clones de volume	Não suportado	
VStorage	Não suportado	A migração não é permitida quando o vStorage está ativado. Para executar uma migração, desative a opção vStorage e, em seguida, reative-a após a conclusão da migração.

Operações compatíveis durante a migração

A tabela a seguir indica operações de volume com suporte à migração do SVM com base no estado de migração:

Operação de volume	Estado de migração do SVM		
	Em andamento	**Em pausa**	* Redução*
Criar	Não é permitido	Permitido	Não suportado
Eliminar	Não é permitido	Permitido	Não suportado
Desativar a análise do sistema de ficheiros	Permitido	Permitido	Não suportado
Análise do sistema de arquivos ativada	Não é permitido	Permitido	Não suportado
Modificar	Permitido	Permitido	Não suportado
Offline/Online	Não é permitido	Permitido	Não suportado
Mover/realojar	Não é permitido	Permitido	Não suportado
Qtree criar/modificar	Não é permitido	Permitido	Não suportado
Quota criar/modificar	Não é permitido	Permitido	Não suportado
Mudar o nome	Não é permitido	Permitido	Não suportado
Redimensionar	Permitido	Permitido	Não suportado
Restringir	Não é permitido	Permitido	Não suportado
Atributos do Snapshot modificam	Permitido	Permitido	Não suportado
snapshot Autodelete Modificar	Permitido	Permitido	Não suportado
Criar Snapshot	Permitido	Permitido	Não suportado
Eliminar instantâneo	Permitido	Permitido	Não suportado
Restaure o arquivo a partir do snapshot	Permitido	Permitido	Não suportado

Migrar um SVM

Após a conclusão da migração para o SVM, os clientes são cortados automaticamente para o cluster de destino e a SVM desnecessária é removida do cluster de origem. A redução automática e a limpeza automática da fonte são ativadas por padrão. Se necessário, você pode desativar a transição automática do cliente para suspender a

migração antes que a transição ocorra e também desativar a limpeza automática da SVM de origem.

- Você pode usar a `-auto-cutover false` opção para suspender a migração quando a transição automática do cliente ocorre normalmente e, em seguida, executar manualmente a transição mais tarde.

  Faça a redução manual dos clientes após a migração do SVM

- Você pode usar a opção de privilégio avançado `-auto-source-cleanup false` para desativar a remoção do SVM de origem após a transição e, em seguida, acionar a limpeza de origem manualmente mais tarde, após a transição.

  Remova manualmente o SVM de origem após a redução

Migrar um SVM com a redução automática habilitada

Por padrão, os clientes são cortados automaticamente para o cluster de destino quando a migração for concluída, e o SVM desnecessário é removido do cluster de origem.

Passos

1. No cluster de destino, execute as verificações prévias de migração:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. No cluster de destino, inicie a migração para o SVM:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name
   ```

3. Verifique o status da migração:

   ```
   dest_cluster> vserver migrate show
   ```

   O status exibe migrar-concluído quando a migração para SVM for concluída.

Migrar um SVM com a redução automática de cliente desativada

Você pode usar a opção -auto-redução false para suspender a migração quando a transição automática do cliente ocorre normalmente e, em seguida, executar manualmente a transição mais tarde. Faça a redução manual dos clientes após a migração do SVMConsulte .

Passos

1. No cluster de destino, execute as verificações prévias de migração:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. No cluster de destino, inicie a migração para o SVM:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-cutover false
   ```

3. Verifique o status da migração:

   `dest_cluster> vserver migrate show` O status exibe pronto para a transição quando a migração para o SVM concluir as transferências de dados assíncronas, e está pronto para a operação de redução.

Migrar um SVM com a limpeza de origem desativada

Você pode usar a opção false privilégio avançado -auto-source-cleanup para desativar a remoção do SVM de origem após a transição e, em seguida, acionar a limpeza da fonte manualmente mais tarde, após a transição. Remova manualmente o SVM de origemConsulte .

Passos

1. No cluster de destino, execute as verificações prévias de migração:

   ```
   dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. No cluster de destino, inicie a migração para o SVM:

   ```
   dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-source-cleanup false
   ```

3. Verifique o status da migração:

   ```
   dest_cluster*> vserver migrate show
   ```

   O status exibe pronto para limpeza da fonte quando a transição da migração para o SVM está concluída, e está pronto para remover o SVM no cluster de origem.

Monitorar a migração de volume

Além de monitorar a migração geral da SVM com o `vserver migrate show` comando, você pode monitorar o status de migração dos volumes que o SVM contém.

Passos

1. Verificar o status da migração de volume:

   ```
   dest_clust> vserver migrate show-volume
   ```

Pausar e retomar a migração da SVM

Talvez você queira pausar uma migração para SVM antes do início da migração. Você pode pausar uma migração SVM usando o `vserver migrate pause` comando.

Pausar a migração

Você pode pausar uma migração SVM antes que a transição do cliente seja iniciada usando o `vserver migrate pause` comando.

Algumas alterações de configuração são restritas quando uma operação de migração está em andamento; no entanto, a partir do ONTAP 9.12,1, você pode pausar uma migração para corrigir algumas configurações

restritas e alguns estados com falha, para que você possa corrigir problemas de configuração que possam ter causado a falha. Alguns dos estados com falha que você pode corrigir ao pausar a migração do SVM incluem o seguinte:

- `setup-configuration-failed`
- `migrate-failed`

Passos

1. A partir do cluster de destino, pause a migração:

```
vserver migrate pause -vserver <vserver name>
```

Retomar migrações

Quando estiver pronto para retomar uma migração SVM pausada ou quando uma migração SVM falhar, você poderá usar o `vserver migrate resume` comando.

Passos

1. Faça o seguinte a partir do cluster de destino:
   a. Retomar a migração da SVM:

```
vserver migrate resume
```

   b. Verifique se a migração do SVM foi retomada e monitore o progresso:

```
vserver migrate show
```

Cancelar uma migração para SVM

Se você precisar cancelar uma migração SVM antes que ela seja concluída, use o `vserver migrate abort` comando. Você pode cancelar uma migração SVM somente quando a operação estiver no estado pausado ou com falha. Você não pode cancelar uma migração para o SVM quando o status for "iniciado na transição" ou após a conclusão da transição. Não é possível usar a `abort` opção quando uma migração para SVM estiver em andamento.

Passos

1. Verifique o status da migração:

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. Cancelar a migração:

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

3. Verifique o andamento da operação de cancelamento:

   ```
   dest_cluster> vserver migrate show
   ```

   O estado de migração mostra migrar-abortar enquanto a operação cancelar está em curso. Quando a operação de cancelamento for concluída, o status de migração não mostra nada.

Cortar manualmente os clientes

Por padrão, a transferência do cliente para o cluster de destino é realizada automaticamente após a migração SVM atingir o estado "pronto para a transição". Se você optar por desativar a transição automática de cliente, precisará executar a transição de cliente manualmente.

Passos

1. Executar manualmente a transição do cliente:

   ```
   dest_cluster> vserver migrate cutover -vserver <vserver name>
   ```

2. Verifique o status da operação de transição:

   ```
   dest_cluster> vserver migrate show
   ```

Remova manualmente o SVM de origem após a transição do cliente

Se você tiver realizado a migração do SVM com a limpeza de origem desativada, poderá remover o SVM de origem manualmente após a conclusão da transferência do cliente.

Passos

1. Verifique se o status deles está pronto para limpeza de origem:

   ```
   dest_cluster> vserver migrate show
   ```

2. Limpe a fonte:

   ```
   dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
   ```

Gerenciamento de par HA

Visão geral do gerenciamento do par HA

Os nós de cluster são configurados em pares de alta disponibilidade (HA) para tolerância de falhas e operações ininterruptas. Se um nó falhar ou se você precisar reduzir um nó para manutenção de rotina, o parceiro poderá assumir o storage e continuar fornecendo dados a partir dele. O parceiro devolve o storage quando o nó é colocado de volta na linha.

A configuração do controlador de par de HA consiste em um par de controladores de storage FAS/AFF

correspondentes (nó local e nó parceiro). Cada um desses nós é conectado às gavetas de disco do outro. Quando um nó em um par de HA encontra um erro e pára o processamento de dados, o parceiro deteta o status com falha do parceiro e assume todo o Data Processing desse controlador.

Takeover é o processo no qual um nó assume o controle do storage de seu parceiro.

Giveback é o processo em que o armazenamento é devolvido ao parceiro.

Por padrão, as aquisições ocorrem automaticamente em qualquer uma das seguintes situações:

- Uma falha de software ou sistema ocorre em um nó que leva a um pânico. Faz failover automático de controladoras de par de HA para o nó de parceiro. Depois que o parceiro se recuperar do pânico e inicializar, o nó automaticamente executa um giveback, retornando o parceiro à operação normal.
- Uma falha do sistema ocorre em um nó e o nó não pode reinicializar. Por exemplo, quando um nó falha devido à perda de energia, os controladores de par de HA fazem failover automático para o nó do parceiro e fornecem dados do controlador de storage que sobreviveu.

> Se o storage de um nó também perder energia ao mesmo tempo, um takeover padrão não será possível.

- As mensagens Heartbeat não são recebidas do parceiro do nó. Isso pode acontecer se o parceiro tiver sofrido uma falha de hardware ou software (por exemplo, uma falha de interconexão) que não resultou em pânico, mas ainda impediu que ele funcionasse corretamente.
- Você interrompe um dos nós sem usar o `-f` parâmetro ou `-inhibit-takeover true`.

> Em um cluster de dois nós com o cluster HA ativado, interromper ou reinicializar um nó usando o `-inhibit-takeover true` parâmetro faz com que ambos os nós parem de fornecer dados, a menos que você primeiro desative a HA do cluster e atribua o epsilon ao nó que você deseja permanecer online.

- Você reinicializa um dos nós sem usar o `-inhibit-takeover true` parâmetro. (O `-onboot` parâmetro `storage failover` do comando está ativado por padrão.)
- O dispositivo de gerenciamento remoto (processador de serviço) deteta falha do nó do parceiro. Isso não se aplica se você desabilitar a aquisição assistida por hardware.

Você também pode iniciar manualmente as aquisições com o `storage failover takeover` comando.

Melhorias no diagnóstico e resiliência do cluster

A partir do ONTAP 9.9,1, as seguintes adições de resiliência e diagnóstico melhoram a operação do cluster:

- **Monitoramento e evitação de portas**: Em configurações de cluster sem switch de dois nós, o sistema evita portas que sofrem perda total de pacotes (perda de conetividade). No ONTAP 9.8,1 e anterior, esta funcionalidade só estava disponível em configurações comutadas.
- * Failover automático de nó*: Se um nó não puder servir dados em sua rede de cluster, esse nó não deve possuir nenhum disco. Em vez disso, seu parceiro de HA deve assumir, se o parceiro for saudável.
- **Comandos para analisar problemas de conetividade**: Use o seguinte comando para exibir quais caminhos de cluster estão enfrentando perda de pacotes: `network interface check cluster-connectivity show`

Como funciona a aquisição assistida por hardware

Habilitado por padrão, o recurso de aquisição assistida por hardware pode acelerar o processo de aquisição usando o dispositivo de gerenciamento remoto de um nó (processador de serviço).

Quando o dispositivo de gerenciamento remoto deteta uma falha, ele inicia rapidamente o takeover em vez de esperar que o ONTAP reconheça que o batimento cardíaco do parceiro parou. Se ocorrer uma falha sem esse recurso ativado, o parceiro espera até que perceba que o nó não está mais dando um heartbeat, confirme a perda de heartbeat e, em seguida, inicie o controle.

O recurso de aquisição assistida por hardware usa o seguinte processo para evitar essa espera:

1. O dispositivo de gerenciamento remoto monitora o sistema local para certos tipos de falhas.
2. Se for detetada uma falha, o dispositivo de gerenciamento remoto enviará imediatamente um alerta ao nó do parceiro.
3. Ao receber o alerta, o parceiro inicia a aquisição.

Eventos do sistema que acionam a aquisição assistida por hardware

O nó do parceiro pode gerar um takeover dependendo do tipo de alerta que recebe do dispositivo de gerenciamento remoto (processador de serviço).

Alerta	Aquisição iniciada após receção?	Descrição
anómala_reboot	Não	Ocorreu uma reinicialização anormal do nó.
l2_watchdog_reset	Sim	O hardware de monitorização do sistema detetou uma reposição L2D. O dispositivo de gerenciamento remoto detetou uma falta de resposta da CPU do sistema e redefiniu o sistema.
loss_of_heartbeat	Não	O dispositivo de gerenciamento remoto não está mais recebendo a mensagem de heartbeat do nó. Este alerta não se refere às mensagens de heartbeat entre os nós no par de HA; refere-se ao heartbeat entre o nó e seu dispositivo de gerenciamento remoto local.
mensagem_periódica	Não	Uma mensagem periódica é enviada durante uma operação normal de aquisição assistida por hardware.
power_cycle_via_SP	Sim	O dispositivo de gerenciamento remoto desligou e ligou o sistema.
power_loss	Sim	Ocorreu uma perda de energia no nó. O dispositivo de gerenciamento remoto possui uma fonte de alimentação que mantém a energia por um curto período após uma perda de energia, permitindo que ele comunique a perda de energia ao parceiro.
power_off_via_SP	Sim	O dispositivo de gerenciamento remoto desligou o sistema.
reset_via_SP	Sim	O dispositivo de gestão remota repõe o sistema.

teste	Não	Uma mensagem de teste é enviada para verificar uma operação de aquisição assistida por hardware.

Informações relacionadas

"Aquisição assistida por hardware (HWassist) - Guia de resolução"

Como a aquisição automática e a giveback funcionam

As operações de aquisição automática e de giveback podem trabalhar em conjunto para reduzir e evitar interrupções do cliente.

Por padrão, se um nó no par de HA ficar em pânico, reinicializa ou pára, o nó do parceiro assume automaticamente o controle e retorna o armazenamento quando o nó afetado é reinicializado. Em seguida, o par de HA retoma um estado operacional normal.

As aquisições automáticas também podem ocorrer se um dos nós não responder.

A giveback automática ocorre por padrão. Se você preferir controlar o impactos da giveback nos clientes, você pode desativar a giveback automática e usar o `storage failover modify -auto-giveback false -node <node>` comando. Antes de executar o giveback automático (independentemente do que o acionou), o nó do parceiro espera por uma quantidade fixa de tempo, conforme controlado pelo `-delay- seconds` parâmetro `storage failover modify` do comando. O atraso padrão é de 600 segundos.

Este processo evita uma interrupção única e prolongada que inclui o tempo necessário para:

- A operação de aquisição
- O nó tomado-over para inicializar até o ponto em que está pronto para o giveback
- A operação de giveback

Se o giveback automático falhar em qualquer um dos agregados não-raiz, o sistema fará automaticamente duas tentativas adicionais para completar o giveback.

Durante o processo de aquisição, o processo automático de giveback começa antes que o nó do parceiro esteja pronto para a giveback. Quando o limite de tempo do processo de giveback automático expirar e o nó do parceiro ainda não estiver pronto, o temporizador será reiniciado. Como resultado, o tempo entre o nó do parceiro estar pronto e o giveback real sendo executado pode ser menor do que o tempo de giveback automático.

O que acontece durante a aquisição

Quando um nó assume o parceiro, ele continua fornecendo e atualizando dados nos agregados e volumes do parceiro.

As etapas a seguir ocorrem durante o processo de aquisição:

1. Se o takeover negociado for iniciado pelo usuário, os dados agregados serão movidos do nó do parceiro para o nó que está realizando o takeover. Uma breve interrupção ocorre quando o proprietário atual de cada agregado (exceto o agregado raiz) muda para o nó de aquisição. Essa interrupção é mais breve do que uma interrupção que ocorre durante uma aquisição sem realocação agregada.

Uma aquisição negociada durante o pânico não pode ocorrer em caso de pânico. Uma aquisição pode resultar de uma falha não associada a um pânico. Uma falha é sentida quando a comunicação é perdida entre um nó e seu parceiro, também chamada de perda de batimento cardíaco. Se um takeover ocorrer por causa de uma falha, a interrupção pode ser maior porque o nó do parceiro precisa de tempo para detectar a perda de batimento cardíaco.

- Você pode monitorar o progresso usando o `storage failover show-takeover` comando.
- Você pode evitar a realocação agregada durante essa instância de aquisição usando o `-bypass -optimization` parâmetro com o `storage failover takeover` comando.

  Os agregados são relocados em série durante operações de aquisição planejadas para reduzir a interrupção do cliente. Se a realocação de agregados for ignorada, uma interrupção mais longa do cliente ocorrerá durante eventos de aquisição planejados.

2. Se o takeover iniciado pelo usuário for um takeover negociado, o nó de destino será desligado graciosamente, seguido do takeover do agregado raiz do nó de destino e de quaisquer agregados que não tenham sido relocados na primeira etapa.
3. As LIFs de dados (interfaces lógicas) migram do nó de destino para o nó de aquisição ou para qualquer outro nó no cluster com base em regras de failover de LIF. Você pode evitar a migração de LIF usando o `-skip-lif-migration` parâmetro com o `storage failover takeover` comando. No caso de uma aquisição iniciada pelo usuário, os LIFs de dados são migrados antes do início da aquisição de storage. Em caso de pânico ou falha, dependendo da sua configuração, os LIFs de dados podem ser migrados com o armazenamento ou após a conclusão da aquisição.
4. As sessões SMB existentes são desconetadas quando ocorre a aquisição.

   Devido à natureza do protocolo SMB, todas as sessões SMB são interrompidas (exceto para sessões SMB 3,0 conetadas a compartilhamentos com o conjunto de propriedades disponibilidade contínua). As sessões SMB 1,0 e SMB 2.x não podem reconetar identificadores de arquivos abertos após um evento de aquisição; portanto, a aquisição é disruptiva e pode ocorrer alguma perda de dados.

5. As sessões SMB 3,0 estabelecidas para compartilhamentos com a propriedade disponibilidade contínua habilitada podem se reconetar aos compartilhamentos desconetados após um evento de aquisição. Se o seu site usar conexões SMB 3,0 com o Microsoft Hyper-V e a propriedade disponibilidade contínua estiver ativada nos compartilhamentos associados, as aquisições não serão disruptivas para essas sessões.

O que acontece se um nó realizar uma pania de aquisição

Se o nó que está executando o painel de controle de aquisição dentro de 60 segundos após o início do controle de aquisição, os seguintes eventos ocorrerão:

- O nó que entrou em pânico reinicializa.
- Após a reinicialização, o nó executa operações de auto-recuperação e não está mais no modo de aquisição.
- O failover está desativado.
- Se o nó ainda possuir alguns agregados do parceiro, depois de ativar o failover de storage, devolva esses agregados ao parceiro usando o `storage failover giveback` comando.

O que acontece durante a giveback

O nó local retorna a propriedade para o nó do parceiro quando os problemas são resolvidos, quando o nó do parceiro é inicializado ou quando a giveback é iniciada.

O seguinte processo ocorre em uma operação normal de giveback. Nesta discussão, o nó A assumiu o nó B. quaisquer problemas no nó B foram resolvidos e está pronto para retomar a distribuição de dados.

1. Quaisquer problemas no nó B são resolvidos e exibe a seguinte mensagem: `Waiting for giveback`
2. A giveback é iniciada pelo `storage failover giveback` comando ou pela giveback automática se o sistema estiver configurado para ele. Isso inicia o processo de retorno da propriedade dos agregados e volumes do nó B do nó A de volta ao nó B.
3. Nó A retorna o controle do agregado raiz primeiro.
4. O nó B completa o processo de inicialização até seu estado operacional normal.
5. Assim que o nó B atinge o ponto no processo de inicialização onde pode aceitar os agregados não-raiz, o nó A retorna a propriedade dos outros agregados, um de cada vez, até que o giveback esteja completo. Você pode monitorar o progresso do giveback usando o `storage failover show-giveback` comando.

> O `storage failover show-giveback` comando não exibe (nem se destina) informações sobre todas as operações que ocorrem durante a operação de failover de armazenamento. Você pode usar o `storage failover show` comando para exibir detalhes adicionais sobre o status de failover atual do nó, como se o nó estiver totalmente funcional, o controle for possível e o giveback estiver concluído.

   E/S é retomado para cada agregado depois que a giveback é concluída para esse agregado, o que reduz sua janela de interrupção geral.

Política DE HA e seu efeito sobre a aquisição e a giveback

A ONTAP atribui automaticamente uma política de HA de CFO (failover de controladora) e SFO (failover de storage) a um agregado. Essa diretiva determina como as operações de failover de storage ocorrem para o agregado e seus volumes.

As duas opções, CFO e SFO, determinam a sequência de controle agregado que o ONTAP usa durante operações de failover de armazenamento e operações de giveback.

Embora os termos CFO e SFO às vezes sejam usados informalmente para se referir a operações de failover de storage (takeover e giveback), eles realmente representam a política de HA atribuída aos agregados. Por exemplo, os termos SFO Aggregate ou CFO Aggregate referem-se simplesmente à atribuição de política de HA do agregado.

As políticas DE HA afetam as operações de aquisição e giveback da seguinte forma:

- Agregados criados em sistemas ONTAP (exceto para o agregado raiz que contém o volume raiz) têm uma política de HA de SFO. A aquisição iniciada manualmente é otimizada para o desempenho relocando agregados SFO (não-raiz) em série para o parceiro antes da aquisição. Durante o processo de giveback, os agregados são devolvidos em série após o arranque do sistema retomado e as aplicações de gestão ficarem online, permitindo que o nó receba os seus agregados.
- Como as operações de realocação de agregados implicam a reatribuição da propriedade de disco agregado e a mudança de controle de um nó para seu parceiro, apenas agregados com uma política de

HA de SFO podem ser qualificados para realocação de agregados.

- O agregado raiz sempre tem uma política de HA de CFO e é devolvido no início da operação de giveback. Isto é necessário para permitir que o sistema tomado-over seja inicializado. Todos os outros agregados são entregues em série depois que o sistema retomado conclui o processo de inicialização e os aplicativos de gerenciamento ficam online, permitindo que o nó receba seus agregados.

> Alterar a política de HA de um agregado de SFO para CFO é uma operação de modo de manutenção. Não modifique esta definição, a menos que seja direcionado para o fazer por um representante do apoio ao cliente.

Como as atualizações em segundo plano afetam a aquisição e a giveback

As atualizações em segundo plano do firmware do disco afetarão as operações de aquisição de par de HA, giveback e realocação agregada de maneira diferente, dependendo de como essas operações são iniciadas.

A lista a seguir descreve como as atualizações de firmware de disco em segundo plano afetam a aquisição, a giveback e a realocação de agregados:

- Se ocorrer uma atualização de firmware de disco em segundo plano em um disco em qualquer nó, as operações de aquisição iniciadas manualmente serão atrasadas até que a atualização de firmware de disco seja concluída nesse disco. Se a atualização de firmware do disco em segundo plano demorar mais de 120 segundos, as operações de aquisição são abortadas e têm de ser reiniciadas manualmente após a conclusão da atualização do firmware do disco. Se o controle tiver sido iniciado com o `-bypass -optimization` parâmetro do `storage failover takeover` comando definido como `true`, a atualização de firmware do disco em segundo plano que ocorre no nó de destino não afetará o controle.
- Se uma atualização de firmware de disco em segundo plano estiver ocorrendo em um disco no nó de origem (ou aquisição) e o controle tiver sido iniciado manualmente com o `-options` parâmetro do `storage failover takeover` comando definido como `immediate`, as operações de aquisição serão iniciadas imediatamente.
- Se uma atualização de firmware de disco em segundo plano estiver ocorrendo em um disco em um nó e ela entrar em pânico, o controle do nó em pânico começará imediatamente.
- Se uma atualização de firmware de disco em segundo plano estiver ocorrendo em um disco em qualquer nó, a giveback dos agregados de dados será adiada até que a atualização de firmware de disco seja concluída nesse disco.
- Se a atualização de firmware do disco em segundo plano demorar mais de 120 segundos, as operações de giveback são abortadas e têm de ser reiniciadas manualmente após a conclusão da atualização do firmware do disco.
- Se uma atualização de firmware de disco em segundo plano estiver ocorrendo em um disco em qualquer nó, as operações de realocação de agregados serão atrasadas até que a atualização de firmware de disco seja concluída nesse disco. Se a atualização do firmware do disco em segundo plano demorar mais de 120 segundos, as operações de realocação agregada serão abortadas e deverão ser reiniciadas manualmente após a conclusão da atualização do firmware do disco. Se a realocação de agregados tiver sido iniciada com o `-override-destination-checks` `storage aggregate relocation` comando definido como `true`, a atualização de firmware do disco em segundo plano que ocorre no nó de destino não afetará a realocação de agregados.

Comandos de takeover automático

A aquisição automática é ativada por padrão em todas as plataformas NetApp FAS, AFF e ASA compatíveis. Talvez seja necessário alterar o comportamento e o controle padrão

quando ocorrem aquisições automáticas quando o nó do parceiro reinicializa, entra em pânico ou pára.

Se você quiser que o controle ocorra automaticamente quando o nó do parceiro…	Use este comando…
Reinicializa ou pára	`storage failover modify -node nodename -onreboot true`
Pânico	`storage failover modify -node nodename -onpanic true`

Ative a notificação por e-mail se a capacidade de aquisição estiver desativada

Para receber uma notificação imediata se o recurso de aquisição for desativado, você deve configurar o sistema para ativar a notificação automática por e-mail para as mensagens EMS "'impossível de aquisição":

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

Comandos automáticos de giveback

Por padrão, o nó de parceiro de tomada de controle automaticamente devolve o armazenamento quando o nó off-line é colocado de volta na linha, restaurando assim a relação de par de alta disponibilidade. Na maioria dos casos, este é o comportamento desejado. Se você precisar desativar a giveback automática - por exemplo, se você quiser investigar a causa da aquisição antes de devolver - você precisa estar ciente da interação de configurações não padrão.

Se você quiser…	Use este comando…
Ative a giveback automática para que a giveback ocorra assim que o nó de tomada de posse for inicializado, atinja o estado de espera por Giveback e o atraso antes do período de retorno automático expirar. A configuração padrão é true.	`storage failover modify -node` *`nodename`* `-auto-giveback true`

Desativar a giveback automática. A configuração padrão é true. **Nota:** a definição deste parâmetro como false não desativa a giveback automática após a aquisição em pânico; a opção automática de domínio após a aquisição em pânico deve ser desativada definindo o `-auto-giveback-after-panic` parâmetro como false.	`storage failover modify -node` *`nodename`* `-auto-giveback false`
Desativar a giveback automática após a aquisição em pânico (esta definição está ativada por predefinição).	`storage failover modify -node` *`nodename`* `-auto-giveback-after-panic false`
Atrasar a giveback automática por um determinado número de segundos (o padrão é 600). Essa opção determina o tempo mínimo que um nó permanece no takeover antes de executar um giveback automático.	`storage failover modify -node` *`nodename`* `-delay-seconds` *`seconds`*

Como as variações do comando de modificação de failover de armazenamento afetam a giveback automática

A operação de giveback automático depende de como você configura os parâmetros do comando de modificação de failover de armazenamento.

A tabela a seguir lista as configurações padrão para os `storage failover modify` parâmetros de comando que se aplicam a eventos de controle não causados por um pânico.

Parâmetro	Predefinição
`-auto-giveback` *true*	*false*`
`true`	`-delay-seconds` *`integer`* `(seconds)`
600	`-onreboot` *true*
false`	*`true`*

A tabela a seguir descreve como as combinações dos `-onreboot` parâmetros e `-auto-giveback` afetam a giveback automática para eventos de aquisição não causados por pânico.

`storage failover modify` parâmetros utilizados	Causa da aquisição	Ocorre giveback automático?
`-onreboot` *`true`* `-auto-giveback` *`true`*	reinicie o comando	Sim

Comando de parada, ou operação do ciclo de energia emitida pelo processador de serviço	Sim	`-onreboot` *`true`* `-auto-giveback` *`false`*
reinicie o comando	Sim	Comando de parada, ou operação do ciclo de energia emitida pelo processador de serviço
Não	`-onreboot` *`false`* `-auto-giveback` *`true`*	reinicie o comando
N/A neste caso, a aquisição não ocorre	Comando de parada, ou operação do ciclo de energia emitida pelo processador de serviço	Sim
`-onreboot` *`false`* `-auto-giveback` *`false`*	reinicie o comando	Não

O `-auto-giveback` parâmetro controla giveback após pânico e todas as outras tomadas automáticas. Se o `-onreboot` parâmetro estiver definido como `true` e ocorrer uma aquisição devido a uma reinicialização, a execução automática da giveback será sempre realizada, independentemente de o `-auto-giveback` parâmetro estar definido como `true`.

O `-onreboot` parâmetro aplica-se a reinicializações e comandos de parada emitidos a partir do ONTAP. Quando o `-onreboot` parâmetro é definido como false, um controle não ocorre no caso de uma reinicialização de nó. Portanto, a giveback automática não pode ocorrer, independentemente de o `-auto-giveback` parâmetro estar definido como true. Ocorre uma interrupção do cliente.

Os efeitos de combinações automáticas de parâmetros de giveback que se aplicam a situações de pânico.

A tabela a seguir lista os `storage failover modify` parâmetros de comando que se aplicam a situações de pânico:

Parâmetro	Predefinição
`-onpanic _true	false_`
`true`	`-auto-giveback-after-panic _true`
false_` (Privilégio: Avançado)	*`true`*
`-auto-giveback _true	false_`

A tabela a seguir descreve como as combinações de parâmetros `storage failover modify` do comando afetam a giveback automática em situações de pânico.

`storage failover` parâmetros utilizados	A giveback automática ocorre após o pânico?

`-onpanic true`
`-auto-giveback true`
`-auto-giveback-after-panic true`
	Sim

`-onpanic true`
`-auto-giveback true`
`-auto-giveback-after-panic false`
	Sim

`-onpanic true`
`-auto-giveback false`
`-auto-giveback-after-panic true`
	Sim

`-onpanic true`
`-auto-giveback false`
`-auto-giveback-after-panic false`
	Não

`-onpanic false` Se `-onpanic` estiver definido como `false`, a aquisição/giveback não ocorrerá, independentemente do valor definido para `-auto-giveback` ou `-auto-giveback-after-panic`	Não

Uma aquisição pode resultar de uma falha não associada a um pânico. Uma *falha* é experimentada quando a comunicação é perdida entre um nó e seu parceiro, também chamada de *perda de heartbeat*. Se uma aquisição ocorrer devido a uma falha, a giveback é controlada pelo `-onfailure` parâmetro em vez do `-auto-giveback-after-panic parameter`.

Quando um nó entra em pânico, ele envia um pacote de pânico para seu nó parceiro. Se, por qualquer motivo, o pacote de pânico não for recebido pelo nó do parceiro, o pânico pode ser mal interpretado como uma falha. Sem o recebimento do pacote de pânico, o nó do parceiro sabe apenas que a comunicação foi perdida e não sabe que ocorreu um pânico. Neste caso, o nó parceiro processa a perda de comunicação como uma falha em vez de um pânico, e a giveback é controlada pelo `-onfailure` parâmetro (e não pelo `-auto-giveback-after-panic parameter`).

Para obter detalhes sobre todos `storage failover modify` os parâmetros, consulte "Páginas de manual do ONTAP".

Comandos de aquisição manual

Você pode executar uma aquisição manualmente quando a manutenção for necessária no parceiro e em outras situações semelhantes. Dependendo do estado do parceiro, o comando que você usa para executar a aquisição varia.

Se você quiser…	Use este comando…
Assuma o nó de parceiro	`storage failover takeover`
Monitore o progresso da takeover à medida que os agregados do parceiro são movidos para o nó fazendo o takeover	`storage failover show-takeover`

Exibir o status de failover de storage para todos os nós no cluster	`storage failover show`
Assuma o nó de parceiro sem migrar LIFs	`storage failover takeover -skip-lif -migration-before-takeover true`
Assuma o nó do parceiro, mesmo que haja uma incompatibilidade de disco	`storage failover takeover -skip-lif -migration-before-takeover true`
Assuma o nó do parceiro mesmo que haja uma incompatibilidade de versão do ONTAP **Observação:** essa opção só é usada durante o processo de atualização do ONTAP sem interrupções.	`storage failover takeover -option allow -version-mismatch`
Assuma o nó de parceiro sem realizar a realocação de agregados	`storage failover takeover -bypass -optimization true`
Assuma o nó de parceiro antes que o parceiro tenha tempo para fechar seus recursos de storage com simplicidade	`storage failover takeover -option immediate`

Antes de emitir o comando de failover de armazenamento com a opção imediata, você deve migrar as LIFs de dados para outro nó usando o seguinte comando: `network interface migrate-all -node` *`node`*

Se você especificar o `storage failover takeover -option immediate` comando sem primeiro migrar as LIFs de dados, a migração de LIF de dados do nó será significativamente adiada mesmo que a `skip-lif-migration-before-takeover` opção não seja especificada.

Da mesma forma, se você especificar a opção imediata, a otimização de aquisição negociada será ignorada mesmo que a opção de otimização de desvio esteja definida como *false*.

Mover o epsilon para certas aquisições iniciadas manualmente

Você deve mover o epsilon se esperar que qualquer aquisição iniciada manualmente possa resultar em uma falha inesperada de nó do sistema de armazenamento longe de uma perda de quorum em todo o cluster.

Sobre esta tarefa

Para realizar a manutenção planejada, você precisa assumir o controle de um dos nós de um par de HA. O quorum em todo o cluster deve ser mantido para evitar interrupções não planejadas de dados do cliente para os nós restantes. Em alguns casos, executar o takeover pode resultar em um cluster que é uma falha inesperada de nó longe da perda de quorum em todo o cluster.

Isso pode ocorrer se o nó que está sendo tomado contém epsilon ou se o nó com epsilon não estiver saudável. Para manter um cluster mais resiliente, é possível transferir o epsilon para um nó íntegro que não está sendo assumido. Normalmente, esse seria o parceiro de HA.

Somente nós saudáveis e elegíveis participam da votação do quórum. Para manter o quórum em todo o cluster, são necessários mais de N/2 votos (onde *N* representa a soma de nós on-line saudáveis e elegíveis). Em clusters com um número par de nós on-line, o epsilon adiciona peso de votação adicional para manter o quórum para o nó ao qual é atribuído.

Embora a votação de formação de cluster possa ser modificada usando o `cluster modify -eligibility false` comando, você deve evitar isso, exceto para situações como restaurar a configuração do nó ou manutenção prolongada do nó. Se você definir um nó como inelegível, ele deixará de fornecer dados SAN até que o nó seja redefinido para elegível e reinicializado. O acesso a dados nas ao nó também pode ser afetado quando o nó não é elegível.

Passos

1. Verifique o estado do cluster e confirme se o epsilon é retido por um nó saudável que não está sendo assumido:

   a. Mude para o nível de privilégio avançado, confirmando que deseja continuar quando o prompt do modo avançado for exibido (*>):

      ```
      set -privilege advanced
      ```

   b. Determine qual nó contém o epsilon:

      ```
      cluster show
      ```

      No exemplo a seguir, Node1 contém epsilon:

Nó	Saúde	Elegibilidade	Epsilon
Node1 Node2	verdadeiro	verdadeiro	verdadeiro falso

   +
   Se o nó que você deseja assumir não tiver o epsilon, avance para o passo 4.

2. Remova o epsilon do nó que você deseja assumir:

   ```
   cluster modify -node Node1 -epsilon false
   ```

3. Atribua o epsilon ao nó do parceiro (neste exemplo, Node2):

   ```
   cluster modify -node Node2 -epsilon true
   ```

4. Realize a operação de aquisição:

   ```
   storage failover takeover -ofnode node_name
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Comandos manuais de giveback

Você pode executar um giveback normal, um giveback no qual você encerra processos no nó do parceiro ou um giveback forçado.

Antes de executar um giveback, é necessário remover as unidades com falha no sistema de tomada a cargo, conforme descrito em "Gerenciamento de discos e agregados".

Se a giveback for interrompida

Se o nó de aquisição sofrer uma falha ou uma interrupção de energia durante o processo de giveback, esse processo pára e o nó de aquisição retorna ao modo de aquisição até que a falha seja reparada ou a energia seja restaurada.

No entanto, isso depende do estágio de giveback em que ocorreu a falha. Se o nó encontrou falha ou uma falha de energia durante o estado parcial de giveback (depois de devolver o agregado raiz), ele não retornará ao modo de aquisição. Em vez disso, o nó retorna ao modo parcial-giveback. Se isso ocorrer, conclua o processo repetindo a operação de giveback.

Se giveback é vetado

Se a giveback for vetada, você deve verificar as mensagens EMS para determinar a causa. Dependendo do motivo ou motivos, você pode decidir se pode substituir os vetos com segurança.

O `storage failover show-giveback` comando exibe o progresso da giveback e mostra qual subsistema vetou a giveback, se houver. Vetos macios podem ser substituídos, enquanto vetos duros não podem ser, mesmo que forçados. As tabelas a seguir resumem os vetos de software que não devem ser substituídos, juntamente com as soluções alternativas recomendadas.

Você pode rever os detalhes do EMS para qualquer vetos de giveback usando o seguinte comando:

```
event log show -node * -event gb*
```

Giveback do agregado raiz

Esses vetos não se aplicam a operações de realocação agregadas:

Módulo do subsistema de veto	Solução alternativa
vfiler_low_level	Encerre as sessões SMB causando o veto ou encerre o aplicativo SMB que estabeleceu as sessões abertas. Substituir esse veto pode fazer com que o aplicativo usando SMB se desconete abruptamente e perca dados.
Verificação do disco	Todos os discos falhados ou ignorados devem ser removidos antes de tentar a giveback. Se os discos estiverem higienizando, aguarde até que a operação seja concluída. Substituir esse veto pode causar uma interrupção causada por agregados ou volumes que ficam offline devido a conflitos de reserva ou discos inacessíveis.

Giveback dos agregados SFO

Esses vetos não se aplicam a operações de realocação agregadas:

Módulo do subsistema de veto	Solução alternativa

Gerenciador de bloqueio	Encerre graciosamente as aplicações SMB que têm arquivos abertos ou mova esses volumes para um agregado diferente. A substituição desse veto resulta na perda do estado de bloqueio SMB, causando interrupções e perda de dados.
LOCK Manager NDESEJA	Aguarde até que os bloqueios sejam espelhados. A substituição desse veto causa interrupções nas máquinas virtuais Microsoft Hyper-V.
RAID	Verifique as mensagens do EMS para determinar a causa do veto: Se o veto for devido ao nvfile, coloque os volumes offline e agregados online. Se as operações de reatribuição de propriedade de disco ou adição de disco estiverem em andamento, aguarde até que elas sejam concluídas. Se o veto for devido a um conflito de nome agregado ou UUID, solucione e o problema. Se o veto for devido a ressincronização do espelho, verificação do espelho ou discos off-line, o veto pode ser substituído e a operação será reiniciada após a giveback.
Inventário de disco	Solucione problemas para identificar e resolver a causa do problema. O nó de destino pode não conseguir ver discos pertencentes a um agregado que está sendo migrado. Discos inacessíveis podem resultar em agregados ou volumes inacessíveis.
Operação de movimentação de volume	Solucione problemas para identificar e resolver a causa do problema. Este veto impede que a operação de movimentação de volume aborte durante a importante fase de transição. Se o trabalho for abortado durante a transição, o volume poderá ficar inacessível.

Comandos para executar um manual giveback

Você pode iniciar manualmente um giveback em um nó em um par de HA para retornar o storage ao proprietário original após concluir a manutenção ou resolver quaisquer problemas que causaram o takeover.

Se você quiser…	Use este comando…
Devolver storage a um nó de parceiro	`storage failover giveback -ofnode` *`nodename`*

Devolva o armazenamento mesmo que o parceiro não esteja no modo de espera para giveback	`storage failover giveback -ofnode` *`nodename`* `-require-partner-waiting false` Não use esta opção a menos que uma interrupção mais longa do cliente seja aceitável.
Devolva o armazenamento mesmo se os processos estiverem vetando a operação de giveback (force a giveback)	`storage failover giveback -ofnode` *`nodename`* `-override-vetoes true` O uso dessa opção pode potencialmente levar a uma falha de cliente mais longa, ou agregados e volumes que não estão online após a giveback.
Devolver apenas os agregados CFO (o agregado raiz)	`storage failover giveback -ofnode` *`nodename`* `-only-cfo-aggregates true`
Monitore o progresso da giveback depois de emitir o comando giveback	`storage failover show-giveback`

Testando a aquisição e a giveback

Depois de configurar todos os aspectos do seu par de HA, você precisa verificar se ele está operando conforme o esperado para manter o acesso ininterrupto ao storage de ambos os nós durante as operações de takeover e giveback. Durante o processo de takeover, o nó local (ou takeover) deve continuar fornecendo os dados normalmente fornecidos pelo nó do parceiro. Durante a giveback, o controle e a entrega do storage do parceiro devem retornar ao nó do parceiro.

Passos

1. Verifique o cabeamento dos cabos de interconexão HA para garantir que eles estejam seguros.
2. Verifique se você pode criar e recuperar arquivos em ambos os nós para cada protocolo licenciado.
3. Introduza o seguinte comando:

   `storage failover takeover -ofnode partnernode`

   Consulte a página man para obter detalhes do comando.

4. Digite um dos seguintes comandos para confirmar que ocorreu a aquisição:

   `storage failover show-takeover`

   `storage failover show`

   Se você tiver `storage failover` a opção do comando `-auto-giveback` ativada:

Nó	Parceiro	Possibilidade de aquisição	Descrição do Estado
nó 1	nó 2	-	À espera de giveback
nó 2	nó 1	falso	Na aquisição, a Auto giveback será iniciada em número de segundos

Se você tiver `storage failover` a opção do comando `-auto-giveback` desativada:

Nó	Parceiro	Possibilidade de aquisição	Descrição do Estado
nó 1	nó 2	-	À espera de giveback
nó 2	nó 1	falso	Na aquisição

5. Exiba todos os discos que pertencem ao nó do parceiro (Node2) que o nó de takeover (Node1) pode detetar:

   `storage disk show -home node2 -ownership`

   O comando a seguir exibe todos os discos pertencentes ao Node2 que o Node1 pode detetar:
   `cluster::> storage disk show -home node2 -ownership`

Disco	Agregado	Casa	Proprietário	DR Home	ID de início	ID do proprietário	ID inicial do DR	Reserver	Piscina
1.0.2	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0

6. Confirme que o nó de takeover (Node1) controla os agregados dos nós de parceiro (Node2):

   `aggr show -fields home-id,home-name,is-home`

agregado	id de casa	casa-namuh	é-casa
aggr0_1	2014942045	node1	verdadeiro
aggr0_2	4078312453	node2	falso
aggr1_1	2014942045	node1	verdadeiro
aggr1_2	4078312453	node2	falso

   Durante a aquisição, o valor "is-home" dos agregados do nó do parceiro é falso.

7. Devolva o serviço de dados do nó do parceiro depois que ele exibe a mensagem "'esperando por

giveback'":

```
storage failover giveback -ofnode partnernode
```

8. Introduza um dos seguintes comandos para observar o progresso da operação de giveback:

```
storage failover show-giveback
```

```
storage failover show
```

9. Prossiga, dependendo se viu a mensagem de que a giveback foi concluída com sucesso:

Se a aquisição e a giveback…	Então…
Foram concluídas com êxito	Repita os passos 2 a 8 no nó do parceiro.
Falha	Corrija a falha de aquisição ou de giveback e, em seguida, repita este procedimento.

Comandos para monitorar um par de HA

Você pode usar comandos ONTAP para monitorar o status do par de HA. Se ocorrer uma aquisição, você também poderá determinar o que causou a aquisição.

Se você quiser verificar	Use este comando
Se o failover está ativado ou ocorreu, ou motivos pelos quais o failover não é possível atualmente	`storage failover show`
Exibir os nós nos quais a configuração de modo de HA de failover de storage está habilitada, você deve definir o valor como HA para o nó participar de uma configuração de failover de storage (par de HA).	`storage failover show -fields mode`
Se a aquisição assistida por hardware está ativada	`storage failover hwassist show`
O histórico de eventos de aquisição assistida por hardware que ocorreram	`storage failover hwassist stats show`
O progresso de uma operação de takeover conforme os agregados do parceiro são movidos para o nó fazendo o takeover	`storage failover show-takeover`
O progresso de uma operação de giveback na devolução de agregados ao nó de parceiro	`storage failover show-giveback`
Se um agregado está em casa durante as operações de aquisição ou de giveback	`aggregate show -fields home-id,owner-id,home-name,owner-name,is-home`
Se a HA do cluster está ativada (aplica-se apenas a dois clusters de nós)	`cluster ha show`
O estado de HA dos componentes de um par de HA (em sistemas que usam o estado de HA)	`ha-config show` Este é um comando do modo de manutenção.

estados de nó exibidos pelos comandos show-type de failover de armazenamento

A lista a seguir descreve os estados do nó que o `storage failover show` comando exibe.

Estado do nó	Descrição
Ligado a Partner_NAME, aquisição automática desativada.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. O takeover automático do parceiro está desativado.
Aguardando pelo Partner_NAME, Giveback dos discos sobressalentes do parceiro pendentes.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA. O reembolso de agregados SFO para o parceiro é feito, mas os discos sobressalentes de parceiros ainda são de propriedade do nó local. • Execute o `storage failover show-giveback` comando para obter mais informações.
A aguardar Partner_NAME. A aguardar a sincronização do bloqueio do parceiro.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA e está aguardando a sincronização do bloqueio do parceiro.
A aguardar Partner_NAME. A aguardar que as aplicações de cluster fiquem online no nó local.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA e está aguardando que os aplicativos de cluster fiquem online.
Takeover agendado. Nó de destino relocando seus agregados SFO na preparação da Takeover.	O processamento de aquisição foi iniciado. O nó de destino está relocando a propriedade de seus agregados SFO em preparação para a aquisição.
O nó de destino realocou seus agregados SFO em preparação para a aquisição.	O processamento de aquisição foi iniciado. O nó de destino relocou a propriedade de seus agregados SFO em preparação para a aquisição.
Takeover agendado. A aguardar para desativar as atualizações de firmware do disco em segundo plano no nó local. Uma atualização de firmware está em andamento no nó.	O processamento de aquisição foi iniciado. O sistema está aguardando a conclusão das operações de atualização de firmware de disco em segundo plano no nó local.
Realocação de agregados SFO para assumir o nó em preparação para a tomada de controle.	O nó local está relocando a propriedade de seus agregados SFO para o nó de aquisição em preparação para o takeover.
Realocaram agregados SFO para o nó de tomada a cargo. Aguardando pela aquisição do nó para o takeover.	A realocação da propriedade de agregados SFO do nó local para o nó de tomada a cargo foi concluída. O sistema está aguardando a aquisição pelo nó de tomada a cargo.

Realocando agregados SFO para Partner_NAME. A aguardar para desativar as atualizações de firmware do disco em segundo plano no nó local. Uma atualização de firmware está em andamento no nó.	A realocação da propriedade de agregados SFO do nó local para o nó de aquisição está em andamento. O sistema está aguardando a conclusão das operações de atualização de firmware de disco em segundo plano no nó local.
Realocando agregados SFO para Partner_NAME. A aguardar para desativar as atualizações de firmware do disco em segundo plano no Partner_NAME. Uma atualização de firmware está em andamento no nó.	A realocação da propriedade de agregados SFO do nó local para o nó de aquisição está em andamento. O sistema está aguardando a conclusão das operações de atualização de firmware de disco em segundo plano no nó do parceiro.
Ligado a Partner_NAME. A tentativa de aquisição anterior foi abortada porque motivo. O nó local possui alguns dos agregados SFO do parceiro. Reemitir uma takeover do parceiro com o `-bypass-optimization` parâmetro definido como true para a aquisição de agregados restantes ou emitir um giveback do parceiro para devolver os agregados transferidos.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. A tentativa de aquisição anterior foi abortada devido ao motivo apresentado em motivo. O nó local possui alguns dos agregados SFO de seu parceiro. • Reemitir um takeover do nó do parceiro, definindo o parâmetro de otimização por desvio como true para takeover dos agregados SFO restantes ou executar um giveback do parceiro para retornar agregados relocados.
Ligado a Partner_NAME. A tentativa de aquisição anterior foi cancelada. O nó local possui alguns dos agregados SFO do parceiro. Reemitir uma takeover do parceiro com o `-bypass-optimization` parâmetro definido como true para a aquisição de agregados restantes ou emitir um giveback do parceiro para devolver os agregados transferidos.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. A tentativa de aquisição anterior foi cancelada. O nó local possui alguns dos agregados SFO de seu parceiro. • Reemitir um takeover do nó do parceiro, definindo o parâmetro de otimização por desvio como true para takeover dos agregados SFO restantes ou executar um giveback do parceiro para retornar agregados relocados.
A aguardar Partner_NAME. A tentativa de aquisição anterior foi abortada porque motivo. O nó local possui alguns dos agregados SFO do parceiro. Reemitir uma takeover do parceiro com o parâmetro "-bypass-optimization" definido como true para a aquisição de agregados restantes, ou emitir um giveback do parceiro para devolver os agregados transferidos.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA. A tentativa de aquisição anterior foi abortada devido ao motivo apresentado em motivo. O nó local possui alguns dos agregados SFO de seu parceiro. • Reemitir um takeover do nó do parceiro, definindo o parâmetro de otimização por desvio como true para takeover dos agregados SFO restantes ou executar um giveback do parceiro para retornar agregados relocados.

A aguardar Partner_NAME. A tentativa de aquisição anterior foi cancelada. O nó local possui alguns dos agregados SFO do parceiro. Reemitir uma takeover do parceiro com o parâmetro "-bypass-optimization" definido como true para a aquisição de agregados restantes, ou emitir um giveback do parceiro para devolver os agregados transferidos.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA. A tentativa de aquisição anterior foi cancelada. O nó local possui alguns dos agregados SFO de seu parceiro. • Reemitir um takeover do nó do parceiro, definindo o parâmetro de otimização por desvio como true para takeover dos agregados SFO restantes ou executar um giveback do parceiro para retornar agregados relocados.
Ligado a Partner_NAME. A tentativa de aquisição anterior foi abortada porque não conseguiu desativar a atualização de firmware do disco em segundo plano (BDFU) no nó local.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. A tentativa de aquisição anterior foi abortada porque a atualização de firmware do disco em segundo plano no nó local não foi desativada.
Ligado a Partner_NAME. A tentativa de aquisição anterior foi abortada porque motivo.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. A tentativa de aquisição anterior foi abortada devido ao motivo apresentado em motivo.
A aguardar Partner_NAME. A tentativa de aquisição anterior foi abortada porque motivo.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA. A tentativa de aquisição anterior foi abortada devido ao motivo apresentado em motivo.
Ligado a Partner_NAME. A tentativa de aquisição anterior por Partner_NAME foi abortada porque motivo.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. A tentativa de aquisição anterior pelo nó do parceiro foi abortada devido ao motivo exibido sob motivo.
Ligado a Partner_NAME. A tentativa de aquisição anterior por Partner_NAME foi abortada.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. A tentativa de aquisição anterior pelo nó do parceiro foi abortada.
A aguardar Partner_NAME. A tentativa de aquisição anterior por Partner_NAME foi abortada porque motivo.	O nó local não pode trocar informações com o nó do parceiro pela interconexão HA. A tentativa de aquisição anterior pelo nó do parceiro foi abortada devido ao motivo exibido sob motivo.
Falha na giveback anterior no módulo: Nome do módulo. Auto giveback será iniciado em segundos.	A tentativa anterior de giveback falhou no módulo module_name. Auto giveback será iniciado em segundos. • Execute o `storage failover show-giveback` comando para obter mais informações.

O nó é proprietário dos agregados do parceiro como parte do procedimento de atualização da controladora sem interrupções.	O nó é proprietário dos agregados de seu parceiro devido ao procedimento de atualização da controladora sem interrupções atualmente em andamento.
Ligado a Partner_NAME. O nó possui agregados pertencentes a outro nó no cluster.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. O nó possui agregados pertencentes a outro nó no cluster.
Ligado a Partner_NAME. A aguardar a sincronização do bloqueio do parceiro.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. O sistema está aguardando a conclusão da sincronização do bloqueio do parceiro.
Ligado a Partner_NAME. A aguardar que as aplicações de cluster fiquem online no nó local.	A interconexão de HA está ativa e pode transmitir dados para o nó do parceiro. O sistema está aguardando que os aplicativos de cluster fiquem online no nó local.
Modo não HA, reinicie para usar o NVRAM completo.	O failover de storage não é possível. A opção de modo HA é configurada como non_ha. • Você deve reinicializar o nó para usar todos os seus NVRAM.
Modo não HA. Reinicie o nó para ativar o HA.	O failover de storage não é possível. • O nó deve ser reinicializado para habilitar a capacidade de HA.
Modo não HA.	O failover de storage não é possível. A opção de modo HA é configurada como non_ha. • Você precisa executar o `storage failover modify -mode ha -node nodename` comando em ambos os nós do par de HA e reinicializar os nós para habilitar a funcionalidade de HA.

Comandos para ativar e desativar o failover de armazenamento

Use os seguintes comandos para ativar e desativar a funcionalidade de failover de armazenamento.

Se você quiser…	Use este comando…
Ativar a aquisição	`storage failover modify -enabled true -node` *`nodename`*
Desativar a aquisição	`storage failover modify -enabled false -node` *`nodename`*

Você só deve desativar o failover de armazenamento se necessário como parte de um procedimento de manutenção.

Interrompa ou reinicie um nó sem iniciar o takeover em um cluster de dois nós

Você interrompe ou reinicializa um nó em um cluster de dois nós sem iniciar o takeover quando executa determinada manutenção de hardware em um nó ou compartimento. Além disso, você deseja limitar o tempo mantendo o nó do parceiro ativo ou quando há problemas para impedir um takeover manual e manter os agregados e fornecendo dados. Além disso, se o suporte técnico estiver ajudando você na solução de problemas, eles podem fazer com que você execute este procedimento como parte desses esforços.

Sobre esta tarefa

- Antes de inibir a aquisição (utilizando o `-inhibit-takeover true` parâmetro), desative a HA do cluster.

  - Em um cluster de dois nós, o cluster HA garante que a falha de um nó não desabilite o cluster. No entanto, se você não desativar a HA do cluster antes de usar o `-inhibit -takeover true` parâmetro, ambos os nós param de fornecer dados.
  - Se você tentar interromper ou reinicializar um nó antes de desativar o HA do cluster, o ONTAP emitirá um aviso e instrui você a desabilitar o HA do cluster.

- Você migra LIFs (interfaces lógicas) para o nó de parceiro que deseja permanecer online.
- Se no nó que você está interrompendo ou reinicializando há agregados que você deseja manter, você os move para o nó que deseja permanecer online.

Passos

1. Verifique se ambos os nós estão íntegros:
   `cluster show`

   Para ambos os nós, `true` aparece `Health` na coluna.

   ```
   cluster::> cluster show
   Node          Health  Eligibility
   ------------ ------- ------------
   node1         true     true
   node2         true     true
   ```

2. Migre todas as LIFs do nó que você interromperá ou reinicializará para o nó do parceiro:
   `network interface migrate-all -node node_name`
3. Se no nó você parar ou reinicializar houver agregados que você deseja manter on-line quando o nó estiver inativo, reposicione-os para o nó do parceiro; caso contrário, vá para a próxima etapa.

   a. Mostrar os agregados no nó que você interromperá ou reiniciará:
      `storage aggregates show -node node_name`

      Por exemplo, node1 é o nó que será interrompido ou reinicializado:

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1       2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
            4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

b. Mova os agregados para o nó de parceiro:
`storage aggregate relocation start -node node_name -destination node_name -aggregate-list aggregate_name`

Por exemplo, agregados aggr1, aggr2 e test2_aggr estão sendo movidos de node1 para node2:

`storage aggregate relocation start -node node1 -destination node2 -aggregate -list aggr1,aggr2,test2_aggr`

4. Desativar cluster HA:
`cluster ha modify -configured false`

A saída de retorno confirma que HA está desativada: `Notice: HA is disabled`

Esta operação não desativa o failover de armazenamento.

5. Interrompa ou reinicie e inibir a aquisição do nó de destino, usando o comando apropriado:
   - `system node halt -node node_name -inhibit-takeover true`
   - `system node reboot -node node_name -inhibit-takeover true`

Na saída do comando, você verá um aviso perguntando se deseja continuar, digite `y`.

6. Verifique se o nó que ainda está on-line está em um estado saudável (enquanto o parceiro está inativo):
`cluster show`

Para o nó on-line, `true` aparece `Health` na coluna.

> Na saída do comando, você verá um aviso de que o cluster HA não está configurado. Neste momento, pode ignorar o aviso.

7. Execute as ações necessárias para interromper ou reinicializar o nó.
8. Inicialize o nó desalinhado a partir do prompt DO Loader:
   `boot_ontap`
9. Verifique se ambos os nós estão íntegros:
   `cluster show`

   Para ambos os nós, `true` aparece `Health` na coluna.

   > Na saída do comando, você verá um aviso de que o cluster HA não está configurado. Neste momento, pode ignorar o aviso.

10. Reative o cluster HA:
    `cluster ha modify -configured true`
11. Se anteriormente neste procedimento você realocou agregados para o nó de parceiro, mova-os de volta para o nó inicial; caso contrário, vá para a próxima etapa:
    `storage aggregate relocation start -node` *`node_name`* `-destination` *`node_name`* `-aggregate-list` *`aggregate_name`*

    Por exemplo, agregados aggr1, aggr2 e test2_aggr estão sendo movidos do nó node2 para o nó node1:
    `storage aggregate relocation start -node` *`node2`* `-destination` *`node1`* `-aggregate -list` *`aggr1`*`,`*`aggr2`*`,`*`test2_aggr`*
12. Reverter LIFs para suas portas domésticas:
    a. Veja LIFs que não estão em casa:
       `network interface show -is-home false`
    b. Se houver LIFs não residenciais que não foram migrados do nó para baixo, verifique se é seguro movê-los antes de reverter.
    c. Se for seguro fazê-lo, reverta todos os LIFs para casa.
       `network interface revert *`

Gerenciamento de API REST com o System Manager

Gerenciamento de API REST com o System Manager

O log da API REST captura as chamadas de API que o Gerenciador de sistema emite para o ONTAP. Você pode usar o log para entender a natureza e a sequência das chamadas necessárias para executar as várias tarefas administrativas do ONTAP.

Como o System Manager usa a API REST e o log de API

Existem várias maneiras pelas quais as chamadas de API REST são emitidas pelo Gerenciador de sistemas para o ONTAP.

Quando o System Manager emite chamadas de API

Aqui estão os exemplos mais importantes de quando o Gerenciador de sistema emite chamadas de API REST do ONTAP.

Atualização automática de página

O System Manager emite automaticamente chamadas de API em segundo plano para atualizar as informações exibidas, como na página do painel.

Exibir ação pelo usuário

Uma ou mais chamadas de API são emitidas quando você exibe um recurso de armazenamento específico ou um conjunto de recursos da IU do System Manager.

Ação de atualização pelo utilizador

Uma chamada de API é emitida quando você adiciona, modifica ou exclui um recurso do ONTAP da IU do Gerenciador do sistema.

Reemitindo uma chamada de API

Você também pode reemitir manualmente uma chamada de API clicando em uma entrada de log. Isso exibe a saída JSON bruta da chamada.

Mais informações

- "Documentos de automação da ONTAP 9"

Acessando o log da API REST

Você pode acessar o log que contém um Registro das chamadas de API REST do ONTAP feitas pelo Gerenciador de sistema. Ao exibir o log, você também pode reemitir chamadas de API e revisar a saída.

Passos

1. Na parte superior da página, clique  para exibir o log da API REST.

   As entradas mais recentes são exibidas na parte inferior da página.

2. À esquerda, clique em **DASHBOARD** e observe as novas entradas que estão sendo criadas para as chamadas de API emitidas para atualizar a página.
3. Clique em **STORAGE** e, em seguida, clique em **Qtrees**.

   Isso faz com que o System Manager emita uma chamada de API específica para recuperar uma lista de Qtrees.

4. Localize a entrada de log descrevendo a chamada API que tem o formulário:

   ```
   GET /api/storage/qtrees
   ```

   Você verá parâmetros de consulta HTTP adicionais incluídos com a entrada, `max_records` como .

5. Clique na entrada de log para reemitir a chamada GET API e exibir a saída JSON bruta.

Exemplo


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
00a0986abd71/1"
        }
      }
```

```
    },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```

Administração de volumes

Gerenciamento de volume e LUN com o System Manager

Visão geral da administração de volumes com o System Manager

A partir do ONTAP 9.7, você pode usar o Gerenciador de sistema para gerenciar o storage lógico, como volumes e LUNs do FlexVol, qtrees, eficiência de storage e cotas.

Se você estiver usando o Gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e anterior), consulte "Gerenciamento do storage lógico"

Gerenciar volumes

Visão geral do gerenciamento de volumes

Depois de exibir uma lista de volumes no System Manager, você pode executar várias ações para gerenciar os volumes.

Passos

1. No System Manager, clique em **Storage > volumes**.

   É apresentada a lista de volumes.

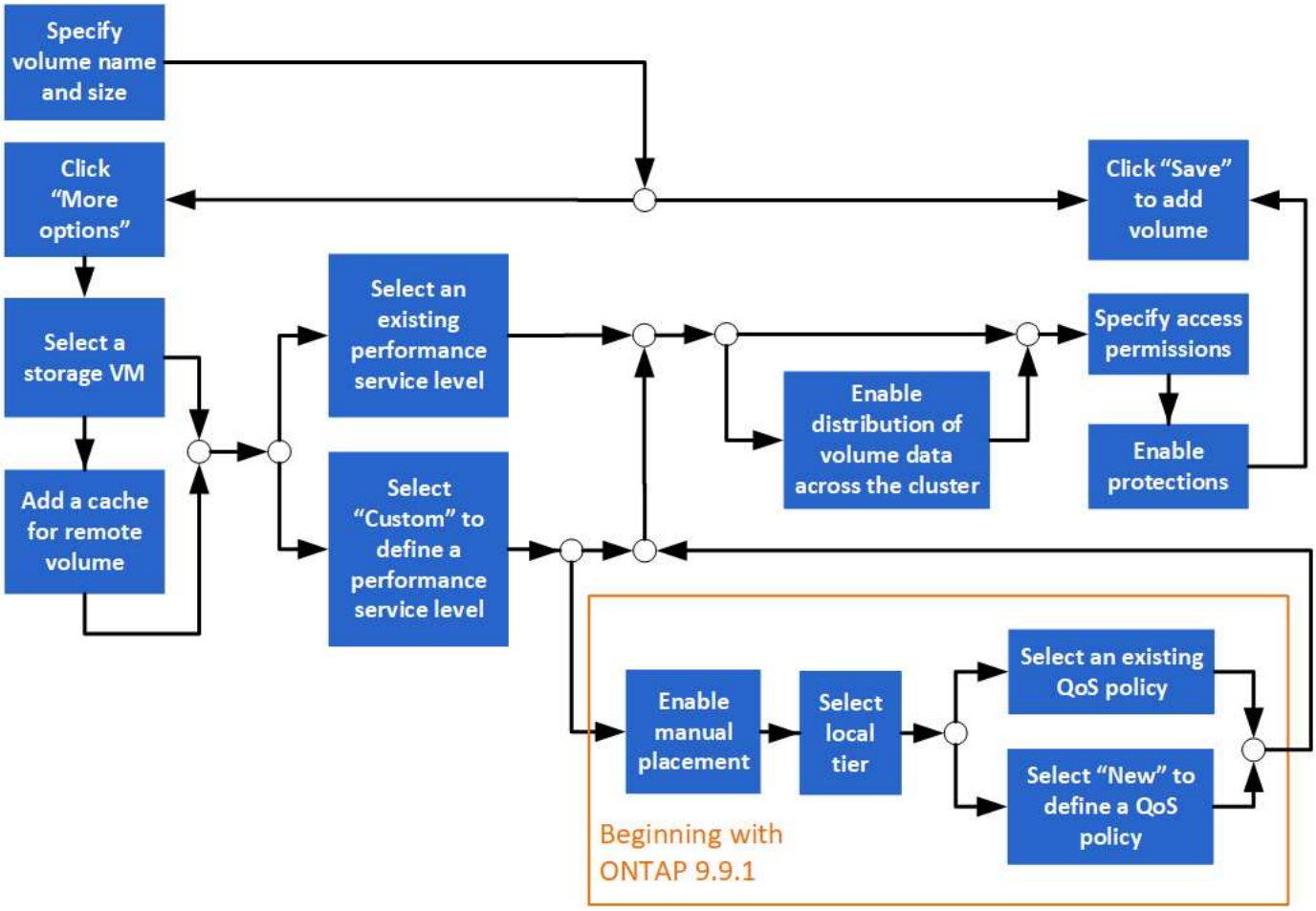
2. Você pode executar o seguinte:

Para executar esta tarefa…	Tome essas ações…
Adicione um volume	Clique + Add em . "Adicione um volume"Consulte .
Gerenciar vários volumes	Marque as caixas ao lado dos volumes. • Clique Delete para eliminar os volumes selecionados. • Clique Protect para atribuir uma política de proteção aos volumes selecionados. • Clique More para selecionar uma das seguintes ações a serem executadas para todos os volumes selecionados: ◦ Ativar quota ◦ Fique offline ◦ Mover ◦ Mostrar volumes eliminados

Gerenciar um único volume	Ao lado do volume, clique em e selecione uma das seguintes ações a serem executadas: • Editar • Redimensionar (começando com ONTAP 9.10,1 e somente para volumes on-line e volumes DP FlexVol) • Eliminar • Clone • Tomar off-line (ou trazer on-line) • Ativar quota (ou Desativar quota) • Editar política de exportação • Editar caminho de montagem • Mover • Edite as configurações do Cloud Tier • Proteger
Renomeie um volume	Pode mudar o nome de um volume a partir da página de descrição geral. Clique ao lado do nome do volume e, em seguida, modifique o nome do volume.

Adicione um volume

Você pode criar um volume e adicioná-lo a uma VM de storage existente que esteja configurada para o serviço NFS ou SMB.



Antes de começar

- Uma VM de storage configurada para serviço NFS ou SMB deve existir no cluster.
- A partir do ONTAP 9.13,1, você pode habilitar a análise de capacidade e o acompanhamento de atividades por padrão em novos volumes. No System Manager, você pode gerenciar as configurações padrão no nível de cluster ou VM de armazenamento. Para obter mais informações, "Ative a análise do sistema de ficheiros"consulte .

Passos

1. Aceda a **armazenamento > volumes**.
2. + Add Selecione .
3. Especifique um nome e tamanho para o volume.
4. Execute um dos seguintes passos:

Selecione este botão…	Para executar esta ação…
Guardar	O volume é criado e adicionado usando os padrões do sistema. Não são necessários passos adicionais.
Mais opções	Avance para para para Etapa 5definir as especificações do volume.

5. o nome e o tamanho do volume são mostrados se você os especificou anteriormente. Caso contrário, introduza o nome e o tamanho.
6. Selecione uma VM de armazenamento na lista suspensa.

Somente as VMs de storage configuradas com o protocolo NFS são listadas. Se apenas uma VM de armazenamento configurada com o protocolo NFS estiver disponível, o campo **Storage VM** não será exibido.

7. Para adicionar um cache para o volume remoto, selecione **Adicionar um cache para o volume remoto** e especifique os seguintes valores:
   - Selecione um cluster.
   - Selecione uma VM de storage.
   - Selecione o volume que pretende ser um volume de cache.
8. Na seção **armazenamento e Otimização**, especifique os seguintes valores:
   a. A capacidade do volume já é mostrada, mas você pode modificá-lo.
   b. No campo **nível de serviço de desempenho**, selecione um nível de serviço:

Ao selecionar este nível de serviço…	Isso ocorre…
Um nível de serviço existente, como "Extreme", "Performance" ou "Value". Somente os níveis de serviço válidos para a plataforma do sistema (AFF, FAS ou outros) são exibidos.	Um nível local ou níveis são escolhidos automaticamente. Prossiga para Etapa 9.
Personalizado	Avance para para para passo 8cdefinir um novo nível de serviço.

   c. começando com o ONTAP 9.9,1, você pode usar o Gerenciador do sistema para selecionar manualmente o nível local no qual deseja colocar o volume que você está criando (se você selecionou o nível de serviço "Personalizado").

> Essa opção não estará disponível se você selecionar **Adicionar como cache para um volume remoto** ou **distribuir dados de volume pelo cluster** (veja abaixo).

Quando você faz esta escolha…	Você executa estes passos…
Colocação manual	A colocação manual está ativada. A seleção **distribuir dados de volume através do cluster** está desativada (veja abaixo). Prossiga para Step 8dconcluir o processo.
Sem seleção	A colocação manual não está ativada. O nível local é selecionado automaticamente. Prossiga para Etapa 9.

   a. Selecione um nível local no menu suspenso.
   b. Selecione uma política de QoS.

      Selecione "existente" para escolher a partir de uma lista de políticas existentes ou selecione "novo" para introduzir as especificações de uma nova política.

9. na seção **Opções de otimização**, determine se você deseja distribuir os dados de volume pelo cluster:

Quando você faz esta escolha…	Isso ocorre…
Distribuir dados de volume pelo cluster	O volume que você está adicionando se torna um volume FlexGroup. Esta opção não está disponível se tiver selecionado anteriormente **colocação manual**.
Sem seleção	O volume que você está adicionando se torna um FlexVol volume por padrão.

10. Na seção **permissões de acesso**, especifique as permissões de acesso para os protocolos para os quais o volume está configurado.

    Começando com ONTAP 9.11,1, o novo volume não será compartilhável por padrão. Você pode especificar as permissões de acesso padrão garantindo que as seguintes caixas de seleção estejam marcadas:

    - **Exportar via NGS**: Cria o volume com a política de exportação "falha" que concede aos usuários acesso total aos dados.
    - **Compartilhar via SMB/CIFS**: Cria um compartilhamento com um nome gerado automaticamente, que você pode editar. O acesso é concedido a "todos". Além disso, você pode especificar o nível de permissão.
11. Na seção **proteção**, especifique as proteções para o volume.
    - A partir do ONTAP 9.12,1, você pode selecionar **Ativar cópias snapshot (local)** e escolher uma política de cópia Snapshot em vez de usar o padrão.
    - Se você selecionar **Enable SnapMirror (local ou remoto)**, especifique a política de proteção e as configurações para o cluster de destino nas listas suspensas.
12. Selecione **Guardar**.

    O volume é criado e adicionado ao cluster e à VM de armazenamento.

> Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Atribuir etiquetas a volumes

A partir do ONTAP 9.14,1, você pode usar o Gerenciador de sistema para atribuir tags a volumes para identificar objetos como pertencentes a uma categoria, como projetos ou centros de custo.

Sobre esta tarefa

Pode atribuir uma etiqueta a um volume. Primeiro, você precisa definir e adicionar a tag. Em seguida, você também pode editar ou excluir a tag.

As tags podem ser adicionadas quando você cria um volume ou podem ser adicionadas mais tarde.

Você define uma tag especificando uma chave e associando um valor a ela usando o formato "chave:valor". Por exemplo: "dept:Engineering" ou "location:san-jose".

O seguinte deve ser considerado quando você cria tags:

- As chaves têm um comprimento mínimo de um caractere e não podem ser nulas. Os valores podem ser nulos.
- Uma chave pode ser emparelhada com vários valores separando os valores com uma vírgula, por exemplo, "'location:san-Jose,toronto'"
- As tags podem ser usadas para vários recursos.
- As teclas devem começar com uma letra minúscula.
- As etiquetas atribuídas aos volumes serão eliminadas quando o volume for eliminado.
- As tags não são recuperadas se um volume for recuperado da fila de recuperação.
- As tags são mantidas se o volume for movido ou clonado.
- As tags atribuídas a VMs de storage em uma relação de recuperação de desastres são replicadas no volume no local do parceiro.

Passos

Para gerenciar tags, execute as seguintes etapas:

1. No System Manager, clique em **volumes** e selecione o volume ao qual deseja adicionar uma tag.

   As tags estão listadas na seção **Tags**.

2. Clique em **Gerenciar tags** para modificar tags existentes ou adicionar novas.

   Você pode adicionar, editar ou excluir as tags.

Para executar esta ação…	Execute estas etapas…
Adicione uma tag	a. Clique em **Add Tag**. b. Especifique uma chave e seu valor ou valores (separe vários valores com vírgulas). c. Clique em **Salvar**.
Edite uma tag	a. Modifique o conteúdo nos campos **Key** e **values (opcional)**. b. Clique em **Salvar**.
Excluir uma tag	a. Clique ao lado da tag que você deseja excluir.

Recuperar volumes excluídos

Se você excluiu acidentalmente um ou mais volumes do FlexVol, use o Gerenciador do sistema para recuperar esses volumes. A partir do ONTAP 9.8, você também pode usar o Gerenciador de sistema para recuperar volumes do FlexGroup. Você também pode excluir os volumes permanentemente limpando os volumes.

O tempo de retenção de volume pode ser definido em um nível de VM de storage. Por padrão, o tempo de retenção do volume é definido para 12 horas.

Selecionar volumes eliminados

Passos

1. Clique em **armazenamento > volumes**.
2. Clique em **mais > Mostrar volumes excluídos**.
3. Selecione os volumes e clique na ação desejada para recuperar ou excluir permanentemente os volumes.

Repor as configurações de volume

A exclusão de um volume exclui as configurações associadas do volume. A recuperação de um volume não repõe todas as configurações. Execute as seguintes tarefas manualmente após recuperar um volume para trazer o volume de volta ao seu estado original:

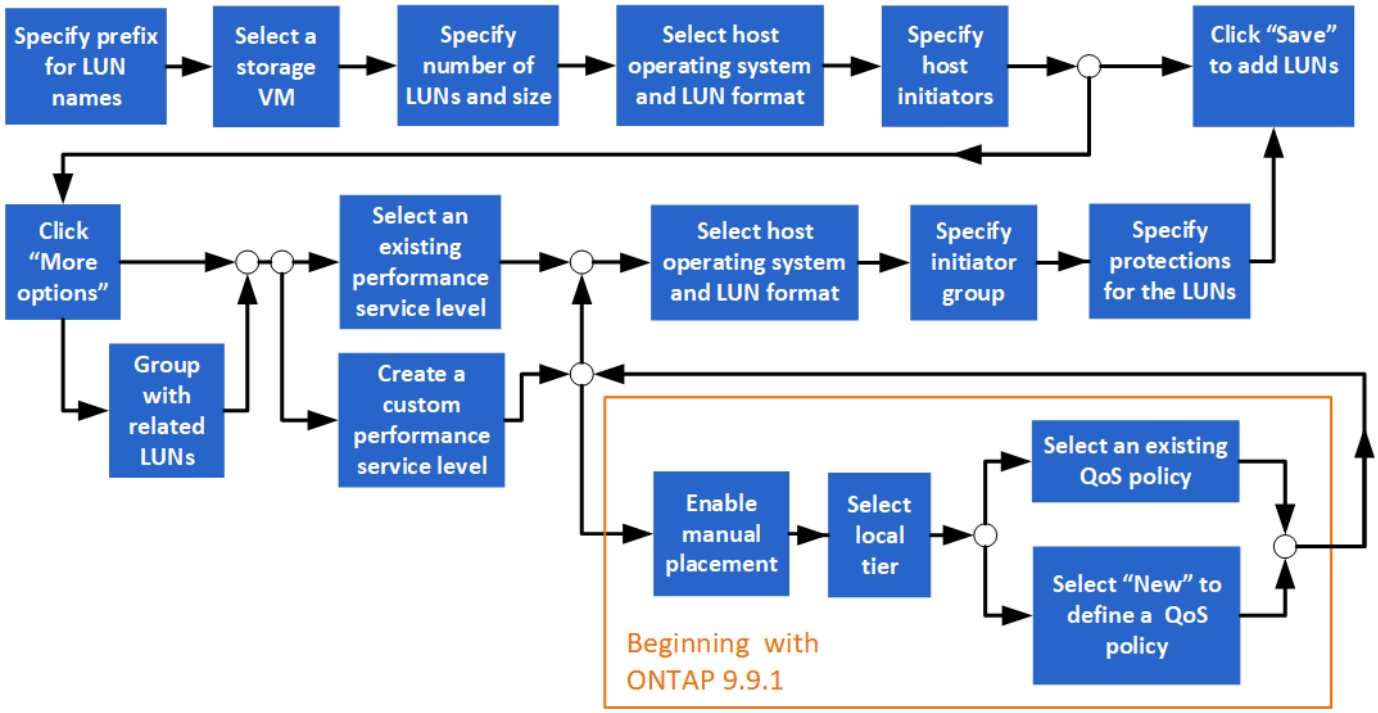
Passos

1. Mude o nome do volume.
2. Configure um caminho de junção (nas).
3. Crie mapeamentos para LUNs no volume (SAN).
4. Associe uma política de snapshot e uma política de exportação ao volume.
5. Adicione novas regras de política de cota para o volume.
6. Adicione uma política DE QOS para o volume.

Gerenciar LUNs

É possível criar LUNs e adicioná-los a uma VM de storage existente configurada com o protocolo SAN. Você também pode agrupar LUNs ou renomeá-los.

Adicionar LUNs



Antes de começar

Uma VM de storage configurada para serviço SAN deve existir no cluster.

Passos

1. Aceda a **armazenamento > LUNs**.
2. Clique + Add em .
3. Especifique um prefixo que será usado no início de cada nome de LUN. (Se você estiver criando apenas um LUN, digite o nome do LUN.)
4. Selecione uma VM de armazenamento na lista suspensa.

   Apenas as VMs de armazenamento configuradas para o protocolo SAN são listadas. Se apenas uma VM de armazenamento configurada para o protocolo SAN estiver disponível, o campo **Storage VM** não será exibido.

5. Indique quantos LUNs pretende criar e o tamanho de cada LUN.
6. Selecione o sistema operacional host e o formato LUN nas listas suspensas.
7. Insira os iniciadores do host e separe-os com vírgulas.
8. Execute uma das seguintes ações:

Clique neste botão…	Para executar esta ação…
Guardar	Os LUNs são criados com as especificações introduzidas. Os padrões do sistema são usados para outras especificações. Não são necessários passos adicionais.
Mais opções	Avance para para para Step 9definir especificações adicionais para os LUNs.

9. o prefixo LUN já é mostrado se você o inseriu anteriormente, mas você pode modificá-lo. Caso contrário, insira o prefixo.
10. Selecione uma VM de armazenamento na lista suspensa.

    Apenas as VMs de armazenamento configuradas para o protocolo SAN são listadas. Se apenas uma VM de armazenamento configurada para o protocolo SAN estiver disponível, o campo **Storage VM** não será exibido.

11. Determine como deseja que os LUNs sejam agrupados:

Quando você faz esta escolha…	Isso ocorre…
Agrupar com LUNs relacionados	Os LUNs serão agrupados com LUNs relacionados em um volume existente na VM de storage.
Sem seleção	Os LUNs serão agrupados em um volume chamado "container".

12. Na seção **armazenamento e Otimização**, especifique os seguintes valores:
    a. O número e a capacidade dos LUNs já são apresentados se os introduziu anteriormente, mas pode modificá-los. Caso contrário, introduza os valores.
    b. No campo **nível de serviço de desempenho**, selecione um nível de serviço:

Ao selecionar este nível de serviço…	Isso ocorre…
Um nível de serviço existente, como "Extreme", "Performance" ou "Value". Somente os níveis de serviço válidos para a plataforma do sistema (AFF, FAS ou outros) são exibidos.	Um nível local é escolhido automaticamente. Prossiga para Etapa 13.
Personalizado	Avance para para para passo 12cdefinir um novo nível de serviço.

c. começando com o ONTAP 9.9,1, você pode usar o Gerenciador do sistema para selecionar manualmente o nível local no qual deseja colocar os LUNs que está criando (se você selecionou o nível de serviço "Personalizado").

Quando você faz esta escolha…	Você executa estes passos…
Colocação manual	A colocação manual está ativada. Prossiga para Step 12dconcluir o processo.
Sem seleção	A seleção manual não está ativada. O nível local é selecionado automaticamente. Prossiga para Etapa 13.

d. Selecione um nível local no menu suspenso.

e. Selecione uma política de QoS.

Selecione "existente" para escolher a partir de uma lista de políticas existentes ou selecione "novo" para introduzir as especificações de uma nova política.

13. na seção **informações do host**, o sistema operacional do host e o formato LUN já são exibidos, mas você pode modificá-los.
14. Em **Host Mapping**, selecione o tipo de iniciadores para os LUNs:
    - **Grupo de iniciadores existente**: Selecione um grupo de iniciadores para a lista exibida.
    - **Novo grupo de iniciadores usando grupos de iniciadores existentes**: Especifique o nome do novo grupo e selecione o grupo ou grupos que deseja usar para criar o novo grupo.
    - **Iniciadores de host**: Especifique um nome do novo grupo de iniciadores e clique em * Adicionar iniciador* para adicionar iniciadores ao grupo.
15. Na seção **proteção**, especifique as proteções para os LUNs.

    Se você selecionar **Enable SnapMirror (local ou remoto)**, especifique a política de proteção e as configurações para o cluster de destino nas listas suspensas.

16. Clique em **Salvar**.

    Os LUNs são criados e adicionados ao cluster e à VM de storage.

Você também pode salvar as especificações desses LUNs em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Renomeie um LUN

Pode mudar o nome de um LUN a partir da página de descrição geral.

Passos

1. No System Manager, clique em **LUNs**.
2. Clique ao lado do nome do LUN que você deseja renomear e, em seguida, modifique o nome do LUN.
3. Clique em **Salvar**.

Expanda o armazenamento

Usando o System Manager, você pode aumentar o tamanho do seu volume ou LUN para que mais espaço esteja disponível para o seu host. O tamanho de um LUN não pode exceder o tamanho do volume que contém.

A partir do ONTAP 9.12,1, quando você insere a nova capacidade de um volume, a janela **Redimensionar volume** exibe o impactos que o redimensionamento do volume terá no espaço de dados e na reserva de cópia Instantânea.

- Aumente o tamanho de um volume
- Aumente o tamanho de um LUN

Além disso, você pode adicionar um LUN a um volume existente. Os processos são diferentes ao usar o Gerenciador de sistemas com o ONTAP 9.7 ou 9,8.

- Adicionar um LUN a um volume existente (ONTAP 9.7)
- Adicionar um LUN a um volume existente (ONTAP 9.8)

Aumente o tamanho de um volume

Passos

1. Clique em **armazenamento > volumes**.
2. Passe o Mouse sobre o nome do volume que você deseja aumentar em tamanho.
3. Clique em .
4. Selecione **Editar**.
5. Aumente o valor da capacidade.
6. Reveja os detalhes do espaço de dados **existente** e **novo** e da reserva de instantâneos.

Aumente o tamanho de um LUN

Passos

1. Clique em **armazenamento > LUNs**.
2. Passe o Mouse sobre o nome do LUN que você deseja aumentar em tamanho.
3. Clique em .
4. Selecione **Editar**.
5. Aumente o valor da capacidade.

Adicionar um LUN a um volume existente (ONTAP 9.7)

Para usar o Gerenciador de sistema com o ONTAP 9.7 para adicionar um LUN a um volume existente, você deve mudar para a Exibição clássica primeiro.

Passos

1. Inicie sessão no Gestor de sistema no ONTAP 9.7.
2. Clique em **Exibição clássica**.
3. Selecione **armazenamento > LUNs > criar**
4. Especifique os detalhes para criar o LUN.
5. Especifique a qual volume ou qtree existente o LUN deve ser adicionado.

Adicionar um LUN a um volume existente (ONTAP 9.8)

A partir do ONTAP 9.8, você pode usar o Gerenciador de sistema para adicionar um LUN a um volume existente que já tenha pelo menos um LUN.

Passos

1. Clique em **armazenamento > LUNs**.
2. Clique em **Adicionar**.
3. Preencha os campos na janela **Add LUNs** (Adicionar LUNs).
4. Selecione **mais opções**.
5. Marque a caixa de seleção **Agrupar com LUNs relacionados**.
6. No campo suspenso, selecione um LUN que existe no volume ao qual você deseja adicionar outro LUN.
7. Preencha o resto dos campos. Para **Host Mapping**, clique em um dos botões de opção:
   - **O grupo de iniciadores existente** permite selecionar um grupo existente de uma lista.
   - **Novo grupo de iniciadores** permite que você insira um novo grupo no campo.

Economizar espaço de storage usando compressão, compactação e deduplicação

Para volumes em clusters que não sejam da AFF, é possível executar deduplicação, compressão de dados e compactação de dados em conjunto ou de forma independente para obter a melhor economia de espaço.

- A deduplicação elimina blocos de dados duplicados.
- A compactação de dados compacta os blocos de dados para reduzir a quantidade de storage físico necessária.
- A compactação de dados armazena mais dados em menos espaço para aumentar a eficiência de storage.

> Essas tarefas são compatíveis com volumes em clusters que não sejam da AFF. A partir do ONTAP 9.2, todos os recursos de eficiência de storage in-line, como deduplicação e compactação in-line, são habilitados por padrão nos volumes AFF.

Passos

1. Clique em **armazenamento > volumes**.

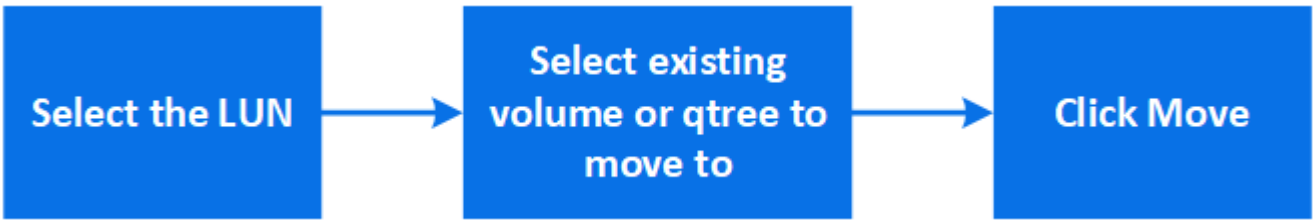
2. Ao lado do nome do volume para o qual você deseja salvar o armazenamento, clique em .
3. Clique em **Editar** e role até **eficiência de armazenamento**.
4. *Opcional*: Se você quiser habilitar a deduplicação em segundo plano, verifique se a caixa de seleção está marcada.
5. *Opcional*: Se você quiser habilitar a compactação em segundo plano, especifique a política de eficiência de armazenamento e verifique se a caixa de seleção está marcada.
6. *Opcional*: Se você quiser ativar a compactação in-line, verifique se a caixa de seleção está marcada.

Equilibre as cargas movendo LUNs

Você pode mover um LUN para outro volume dentro da VM de storage para equilibrar a carga ou movê-lo para um volume com um nível de serviço de performance mais alto para aprimorar a performance.

Mover restrições

- Um LUN não pode ser movido para uma qtree dentro do mesmo volume.
- Um LUN criado a partir de um arquivo usando a CLI não pode ser movido com o System Manager.
- Não é possível mover LUNs on-line e fornecendo dados.
- Os LUNs não podem ser movidos se o espaço alocado no volume de destino não puder conter o LUN (mesmo que o crescimento automático esteja ativado no volume).
- Os LUNs nos volumes SnapLock não podem ser movidos com o Gerenciador do sistema.



Passos

1. Clique em **armazenamento > LUNs**.
2. Selecione o LUN que deseja mover e clique em **mover**.
3. Selecione um volume existente para o qual pretende mover o LUN. Se o volume contiver qtrees, selecione a qtree.

Enquanto a operação de movimentação estiver em andamento, o LUN é exibido no volume de origem e destino.

Equilibre as cargas movendo volumes para outro nível

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para mover um volume para outro nível para equilibrar a carga.

A partir do ONTAP 9.9,1, você também pode mover volumes com base na análise de storage de dados ativo e inativo. Para obter mais informações, "Visão geral do File System Analytics"consulte .

Passos

1. Clique em **armazenamento > volumes**.
2. Selecione o volume ou volumes que deseja mover e clique em **mover**.
3. Selecione um nível existente (agregado) para o qual você deseja mover o volume ou volumes.

Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs

A partir do ONTAP 9.9,1, você pode usar os Playbooks do Ansible com o Gerenciador de sistemas quando quiser adicionar ou editar volumes ou LUNs.

Esse recurso permite que você use a mesma configuração várias vezes ou use a mesma configuração com pequenas alterações ao adicionar ou editar volumes ou LUNs.

Ative ou desative os Playbooks do Ansible

Você pode ativar ou desativar o uso de Playbooks do Ansible com o System Manager.

Passos

1. No System Manager, vá para as configurações da IU na página de configurações do cluster:

   Cluster > Settings

2. Em **Configurações da IU**, altere o interrutor deslizante para "habilitado" ou "Desativado".

Salvar uma configuração de volume em um Playbook do Ansible

Ao criar ou modificar a configuração de um volume, você pode salvar a configuração como arquivos do Ansible Playbook.

Passos

1. Adicionar ou editar o volume:

   Volume > Adicionar (ou **volume > Editar**)

2. Especifique ou edite os valores de configuração do volume.
3. Selecione **Salvar no Ansible Playbook** para salvar a configuração nos arquivos do Ansible Playbook.

   Um arquivo zip é baixado que contém os seguintes arquivos:

   - **`variable.yaml`**: Os valores inseridos ou modificados para adicionar ou editar o volume.
   - **`volumeAdd.yaml`** (Ou **`volumeEdit.yaml`**): Os casos de teste que são necessários para criar ou modificar os valores ao ler as entradas do `variable.yaml` arquivo.

Salve uma configuração LUN em um Playbook do Ansible

Ao criar ou modificar a configuração de um LUN, você pode salvar a configuração como arquivos do Ansible Playbook.

Passos

1. Adicione ou edite o LUN:

LUN > Adicionar (ou **LUN > Editar**)

2. Especifique ou edite os valores de configuração do LUN.
3. Selecione **Salvar no Ansible Playbook** para salvar a configuração nos arquivos do Ansible Playbook:

   Um arquivo zip é baixado que contém os seguintes arquivos:

   - **`variable.yaml`**: Os valores inseridos ou modificados para adicionar ou editar o LUN.
   - **`lunAdd.yaml`** (Ou **`lunEdit.yaml`**): Os casos de teste que são necessários para criar ou modificar os valores ao ler as entradas do `variable.yaml` arquivo.

Baixe arquivos do Ansible Playbook a partir dos resultados de pesquisa global

Você pode baixar arquivos do Ansible Playbook quando fizer uma pesquisa global.

Passos

1. No campo de pesquisa, digite "volume" ou "LUN" ou "Playbook".
2. Encontre o resultado da pesquisa, seja "Gerenciamento de volume (Ansible Playbook)" ou "Gerenciamento de LUN (Ansible Playbook)".
3. Clique em para baixar os arquivos do Ansible Playbook.

Trabalhe com arquivos do Playbook do Ansible

Os arquivos do Ansible Playbook podem ser modificados e executados para especificar configurações para volumes e LUNs.

Sobre esta tarefa

Você usa dois arquivos para executar uma operação (um "adicionar" ou um "editar"):

Se você quiser…	Use este arquivo de variável…	E use este arquivo de execução…
Adicione um volume	`volumeAdd-varible.yaml`	`valueAdd.yaml`
Edite um volume	`volumeEdit-variable.yaml`	`volumeEdit.yaml`
Adicione um LUN	`lunAdd-variable.yaml`	`lunAdd.yaml`
Edite um LUN	`lunEdit-variable.yaml`	`lunEdit.yaml`

Passos

1. Modifique o arquivo de variáveis.

   O arquivo contém os vários valores que você usa para configurar o volume ou LUN.

   - Se você não alterar os valores, deixe-os comentados.
   - Se você modificar os valores, remova os comentários.
2. Execute o arquivo de execução associado.

   O arquivo de execução contém os casos de teste que são necessários para criar ou modificar os valores ao ler as entradas do arquivo variável.

3. Introduza as suas credenciais de início de sessão de utilizador.

Gerenciar políticas de eficiência de storage

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para habilitar, desabilitar, adicionar, editar ou excluir políticas de eficiência para VMs de armazenamento em sistemas FAS.

Esta função não está disponível em sistemas AFF.

Passos

1. Selecione **Storage > Storage VMs**
2. Selecione a VM de storage para a qual deseja gerenciar políticas de eficiência.
3. Na guia **Configurações**, selecione → na seção **Política de eficiência**. As políticas de eficiência dessa VM de storage são exibidas.

Você pode executar as seguintes tarefas:

- **Ativar ou desativar** uma política de eficiência clicando no botão de alternância na coluna Status.
- **Adicione** uma política de eficiência clicando em **Adicionar**.
- **Editar** uma política de eficiência clicando ⋮ à direita do nome da política e selecionando **Editar**.
- **Excluir** uma política de eficiência clicando ⋮ à direita do nome da política e selecionando **Excluir**.

Lista de políticas de eficiência

- **Auto**

  Especifica que a deduplicação é executada continuamente em segundo plano. Essa política é definida para todos os volumes recém-criados e para todos os volumes atualizados que não foram configurados manualmente para deduplicação em segundo plano. Se você alterar a política para "falha" ou qualquer outra política, a política "automática" será desativada.

  Se um volume se mover de um sistema que não seja AFF para um sistema AFF, a política "'auto'" será ativada por padrão no nó de destino. Se um volume passar de um nó AFF para um nó não AFF, a política "'auto'" no nó de destino será substituída pela política "'inline-only'" por padrão.

- **Política**

  Especifica o nome de uma política de eficiência.

- **Status**

  Especifica o status de uma política de eficiência. O status pode ser um dos seguintes:

  - Ativado

    Especifica que a política de eficiência pode ser atribuída a uma operação de deduplicação.

  - Desativado

    Especifica que a política de eficiência está desativada. Você pode ativar a política usando o menu

suspenso status e atribuí-la posteriormente a uma operação de deduplicação.

- **Corra por**

  Especifica se a política de eficiência de storage é executada com base em uma programação ou em um valor de limite (alterar limite de log).

- **Política de QoS**

  Especifica o tipo de QoS para a política de eficiência de storage. O tipo de QoS pode ser um dos seguintes:

  - Fundo

    Especifica que a política de QoS está sendo executada em segundo plano, o que reduz o potencial impactos no desempenho nas operações do cliente.

  - Melhor esforço

    Especifica que a política de QoS está sendo executada com o melhor esforço, o que permite maximizar a utilização de recursos do sistema.

- **Tempo de execução máximo**

  Especifica a duração máxima do tempo de execução de uma política de eficiência. Se esse valor não for especificado, a política de eficiência será executada até que a operação esteja concluída.

Área de detalhes

A área abaixo da lista de políticas de eficiência exibe informações adicionais sobre a política de eficiência selecionada, incluindo o nome da programação e os detalhes da programação de uma política baseada em programação e o valor limite para uma política baseada em limites.

Gerenciar recursos usando cotas

A partir do ONTAP 9.7, você pode configurar e gerenciar cotas de uso com o Gerenciador de sistema.

Se você estiver usando a CLI do ONTAP para configurar e gerenciar cotas de uso, "Gerenciamento de storage lógico"consulte .

Se você estiver usando o OnCommand System Manager legado para ONTAP 9.7 e versões anteriores para configurar e gerenciar cotas de uso, consulte o seguinte para sua versão:

- "Documentação do ONTAP 9 .6 e 9,7"
- "Documentação do ONTAP 9,5"
- "Documentação do ONTAP 9,4"
- "Documentação do ONTAP 9,3"
- "Documentação arquivada do ONTAP 9.2"
- "Documentação arquivada do ONTAP 9.0"

Visão geral da cota

As cotas fornecem uma maneira de restringir ou rastrear o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree. As cotas são aplicadas a um volume ou qtree específico.

Você pode usar cotas para rastrear e limitar o uso de recursos em volumes e fornecer notificações quando o uso de recursos atingir níveis específicos.

As quotas podem ser suaves ou difíceis. As cotas flexíveis fazem com que o ONTAP envie uma notificação quando os limites especificados forem excedidos e as cotas rígidas impedem que uma operação de gravação seja bem-sucedida quando os limites especificados forem excedidos.

Defina cotas para limitar o uso de recursos

Adicione cotas para limitar a quantidade de espaço em disco que o destino de cota pode usar.

Você pode definir um limite rígido e um limite suave para uma cota.

As cotas rígidas impõem um limite rígido aos recursos do sistema; qualquer operação que resultaria em exceder o limite falha. As cotas flexíveis enviam uma mensagem de aviso quando o uso de recursos atinge um determinado nível, mas não afetam as operações de acesso a dados, para que você possa tomar as medidas apropriadas antes que a cota seja excedida.

Passos

1. Clique em **armazenamento > cotas**.
2. Clique em **Add**.

Clonar volumes e LUNs para teste

Você pode clonar volumes e LUNs para criar cópias temporárias e graváveis para teste. Os clones refletem o estado atual e pontual dos dados. Você também pode usar clones para conceder acesso aos dados a outros usuários sem conceder a eles acesso aos dados de produção.

A licença FlexClone deve estar "instalado" no sistema de storage.

Clonar um volume

Crie um clone de um volume, da seguinte forma:

Passos

1. Clique em **armazenamento > volumes**.
2. Clique ⋮ ao lado do nome do volume que deseja clonar.
3. Selecione **Clone** na lista.
4. Especifique um nome para o clone e complete as outras seleções.
5. Clique em **Clone** e verifique se o clone de volume aparece na lista de volumes.

Como alternativa, você pode clonar um volume a partir da **Visão geral** que é exibida quando você visualiza detalhes do volume.

Clonar um LUN

Crie um clone de um LUN, da seguinte forma:

Passos

1. Clique em **armazenamento > LUNs**.
2. Clique ⋮ ao lado do nome do LUN que você deseja clonar.
3. Selecione **Clone** na lista.
4. Especifique um nome para o clone e complete as outras seleções.
5. Clique em **Clone** e verifique se o clone LUN aparece na lista de LUNs.

Como alternativa, você pode clonar um LUN a partir da **Visão geral** que é exibida quando você visualiza os detalhes do LUN.

Quando você cria um clone de LUN, o System Manager ativa automaticamente a exclusão do clone quando o espaço é necessário.

PESQUISE, filtre e classifique informações no System Manager

Você pode pesquisar vários tópicos de ações, objetos e informações no System Manager. Você também pode pesquisar dados da tabela para entradas específicas.

O System Manager fornece dois tipos de pesquisa:

- Pesquisa global

  Quando você insere um argumento de pesquisa no campo na parte superior de cada página, o System Manager pesquisa em toda a interface para encontrar correspondências. Em seguida, você pode classificar e filtrar os resultados.

  A partir do ONTAP 9.12,1, o Gerenciador do sistema também fornece resultados de pesquisa do site de suporte da NetApp para fornecer links para informações de suporte relevantes.

- Pesquisa de tabela-grade

  Começando com ONTAP 9.8, quando você insere um argumento de pesquisa no campo na parte superior de uma grade de tabela, o Gerenciador de sistema pesquisa apenas as colunas e linhas dessa tabela para encontrar correspondências.

Pesquisa global

Na parte superior de cada página do System Manager, você pode usar um campo de pesquisa global para pesquisar vários objetos e ações na interface. Por exemplo, você pode procurar objetos diferentes por nome, páginas disponíveis na coluna do navegador (no lado esquerdo), vários itens de ação, como "Adicionar volume" ou "Adicionar licença" e links para tópicos de ajuda externos. Você também pode filtrar e classificar os resultados.

Para obter melhores resultados, execute a pesquisa, filtragem e classificação um minuto após o login e cinco minutos após criar, modificar ou excluir um objeto.

Obtendo resultados de pesquisa

A pesquisa não é sensível a maiúsculas e minúsculas. Você pode inserir uma variedade de strings de texto para encontrar a página, ações ou tópicos de informações que você precisa. São listados até 20 resultados. Se forem encontrados mais resultados, clique em **Mostrar mais** para ver todos os resultados. Os exemplos a seguir descrevem pesquisas típicas:

Tipo de pesquisa	String de pesquisa de amostra	Exemplos de resultados de pesquisa
Por nome do objeto	vol_	Vol_lun_dest no armazenamento VM: svm0 (volume) /vol/vol… est1/LUN no armazenamento VM: svm0 (LUN) svm0:vol_lun_dest1 função: Destino (relação)
Por localização na interface	volume	Adicionar volume (Ação) proteção – Visão geral (Página) recuperar volume excluído (Ajuda)
Por ações	adicionar	Adicionar volume (Ação) rede – Visão geral (Página) expandir volumes e LUNs (Ajuda)
Por conteúdo de ajuda	san	Armazenamento – Visão geral (Página) Visão geral da SAN (Ajuda) provisão de armazenamento SAN para bancos de dados (Ajuda)

Resultados da pesquisa global a partir do site de suporte da NetApp

A partir do ONTAP 9.12,1, para usuários registrados no Active IQ Digital Advisor (também conhecido como Consultor Digital), o Gerenciador de sistemas exibe outra coluna de resultados que fornece links para informações do site de suporte da NetApp, incluindo informações sobre o produto Gerenciador de sistemas.

Os resultados da pesquisa contêm as seguintes informações:

- **Título** da informação que é um link para o documento em HTML, PDF, EPUB ou outro formato.
- * Tipo de conteúdo*, que identifica se é um tópico de documentação do produto, um artigo da base de conhecimento ou outro tipo de informação.
- **Descrição resumida** do conteúdo.
- **Criado** data em que foi publicado pela primeira vez.
- **Atualizado** data em que foi atualizado pela última vez.

Você pode executar as seguintes ações:

Ação	Resultado
Clique em **Gerenciador do sistema ONTAP** e, em seguida, digite o texto no campo de pesquisa.	Os resultados da pesquisa incluem informações do site de suporte da NetApp sobre o Gerenciador do sistema.

Clique em **todos os produtos** e, em seguida, introduza o texto no campo de pesquisa.	Os resultados da pesquisa incluem informações do site de suporte da NetApp para todos os produtos NetApp, não apenas para o Gerenciador de sistemas.
Clique em um resultado de pesquisa.	As informações do site de suporte da NetApp são exibidas em uma janela ou guia separada do navegador.
Clique em **Veja mais resultados**.	Se houver mais de dez resultados, você pode clicar em **Veja mais resultados** após o décimo resultado para ver mais resultados. Cada vez que você clica em **Veja mais resultados**, outros dez resultados são exibidos, se disponíveis.
Copie o link.	O link é copiado para a área de transferência. Você pode colar o link em um arquivo ou em uma janela do navegador.
Clique em .	O painel onde os resultados são exibidos é fixado para que ele permaneça exibido quando você trabalha em outro painel.
Clique em .	O painel de resultados não está mais fixado e está fechado.

Filtrando os resultados da pesquisa

Você pode restringir os resultados com filtros, como mostrado nos exemplos a seguir:

Filtro	Sintaxe	String de pesquisa de amostra
Por tipo de objeto	<type>:<objectName>	volume:vol_2
Por tamanho do objeto	<type> <size-symbol> <number> <units>	luns clientes 500mb
Por discos quebrados	"disco quebrado" ou "disco não saudável"	disco não saudável
Por interface de rede	<IP address>	172.22.108.21

Ordenar os resultados da pesquisa

Quando você visualiza todos os resultados da pesquisa, eles são ordenados alfabeticamente. Você pode classificar os resultados clicando Filter e selecionando como deseja classificar os resultados.

Pesquisa de tabela-grade

A partir do ONTAP 9.8, sempre que o Gerenciador do sistema exibir informações em um formato de tabela-grade, um botão de pesquisa aparece na parte superior da tabela.

Quando você clica em **pesquisar**, um campo de texto aparece no qual você pode inserir um argumento de pesquisa. O System Manager pesquisa toda a tabela e exibe apenas as linhas que contêm texto que corresponde ao seu argumento de pesquisa.

Você pode usar um asterisco (*) como um caractere "curinga" como um substituto para carateres. Por exemplo, a pesquisa `vol*` pode fornecer linhas que contêm o seguinte:

- vol_122_D9
- vol_lun_dest1
- vol2866
- volspec1
- volum_dest_765
- volume
- volume_new4
- volume9987

Medições de capacidade no System Manager

A capacidade do sistema pode ser medida como espaço físico ou espaço lógico. A partir do ONTAP 9.7, o Gerenciador de sistemas fornece medições de capacidade física e lógica.

As diferenças entre as duas medições são explicadas nas seguintes descrições:

- **Capacidade física**: O espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume ou nível local. O valor da capacidade física usada geralmente é menor do que o valor da capacidade lógica usada devido à redução de dados de recursos de eficiência de storage (como deduplicação e compactação).
- **Capacidade lógica**: O espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume ou nível local. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados da deduplicação ou compressão. O valor do espaço lógico usado é derivado da quantidade de espaço físico usado, além da economia com recursos de eficiência de storage (como deduplicação e compactação) configurados. Essa medição geralmente parece maior do que a capacidade física usada porque inclui cópias Snapshot, clones e outros componentes, e não reflete a compactação de dados e outras reduções no espaço físico. Assim, a capacidade lógica total poderia ser maior do que o espaço provisionado.

No System Manager, as representações de capacidade não são responsáveis pelas capacidades da camada de storage raiz (agregado).

Medições da capacidade utilizada

As medições da capacidade utilizada são apresentadas de forma diferente, dependendo da versão do System Manager que estiver a utilizar, conforme explicado na seguinte tabela:

Versão do System Manager	Termo usado para a capacidade	Tipo de capacidade referida
9.9.1 e mais tarde	Lógica utilizada	Espaço lógico utilizado se as definições de eficiência de armazenamento tiverem sido ativadas)
9,7 e 9,8	Usado	Espaço lógico utilizado (se as definições de eficiência de armazenamento tiverem sido ativadas)

9,5 e 9,6 (vista clássica)	Usado	Espaço físico utilizado

Termos de medição da capacidade

Os seguintes termos são usados ao descrever a capacidade:

- **Capacidade alocada**: A quantidade de espaço que foi alocada para volumes em uma VM de armazenamento.
- **Disponível**: A quantidade de espaço físico disponível para armazenar dados ou provisionar volumes em uma VM de storage ou em um nível local.
- **Capacidade entre volumes**: A soma do armazenamento usado e do armazenamento disponível de todos os volumes em uma VM de armazenamento.
- **Dados do cliente**: A quantidade de espaço usada pelos dados do cliente (físico ou lógico).
  - A partir do ONTAP 9.13,1, a capacidade usada pelos dados do cliente é chamada de **Logical Used**, e a capacidade usada pelas cópias Snapshot é exibida separadamente.
  - No ONTAP 9.12,1 e anterior, a capacidade usada pelos dados do cliente adicionada à capacidade usada pelas cópias Snapshot é referida como **Logical Used**.
- * Comprometido*: O montante da capacidade comprometida para um nível local.
- **Redução de dados**: A relação entre o tamanho dos dados ingeridos e o tamanho dos dados armazenados.
  - A partir do ONTAP 9.13,1, a redução de dados considera os resultados da maioria dos recursos de eficiência de storage, como deduplicação e compactação. No entanto, snapshots e thin Provisioning não são contados como parte da taxa de redução de dados.
  - No ONTAP 9.12,1 e anteriores, as relações de redução de dados são apresentadas da seguinte forma:
    - O valor de redução de dados exibido no painel **capacidade** é a proporção geral de todo o espaço lógico usado em comparação com o espaço físico usado, e inclui os benefícios derivados do uso de cópias Snapshot e outros recursos de eficiência de storage.
    - Quando você exibe o painel de detalhes, você vê a proporção **geral** exibida no painel de visão geral e a proporção do espaço lógico usado somente pelos dados do cliente em comparação com o espaço físico usado somente pelos dados do cliente, conhecido como **sem cópias Snapshot e clones**.
- **Utilização lógica**:
  - A partir do ONTAP 9.13,1, a capacidade usada pelos dados do cliente é chamada de **Logical Used**, e a capacidade usada pelas cópias Snapshot é exibida separadamente.
  - No ONTAP 9.12,1 e anterior, a capacidade usada pelos dados do cliente adicionada à capacidade usada pelas cópias Snapshot é referida como **uso lógico**.
- **% De utilização lógica**: A percentagem da capacidade lógica utilizada atual em comparação com o tamanho provisionado, excluindo reservas de instantâneos. Esse valor pode ser superior a 100%, pois inclui economia de eficiência no volume.
- **Capacidade máxima**: A quantidade máxima de espaço alocada para volumes em uma VM de armazenamento.
- **Físico usado**: A quantidade de capacidade usada nos blocos físicos de um volume ou nível local.
- * % Física usada*: A porcentagem de capacidade usada nos blocos físicos de um volume em comparação com o tamanho provisionado.

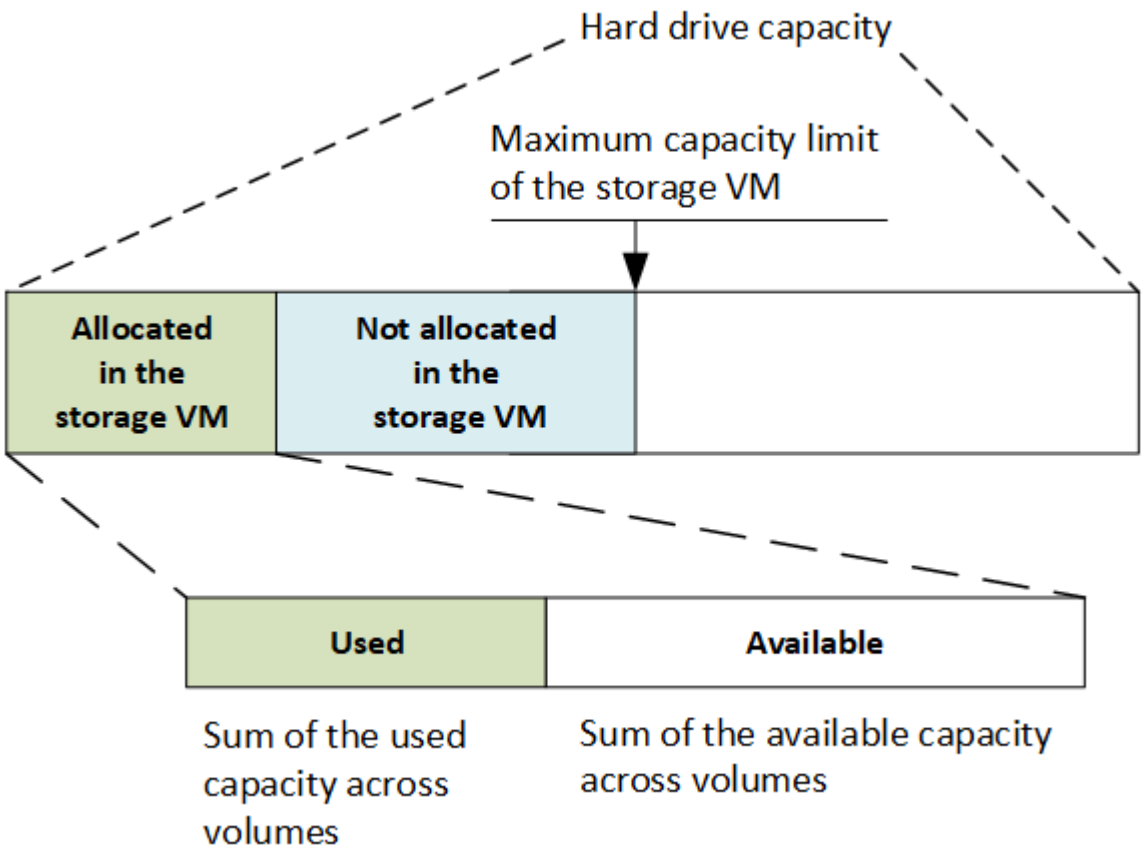
- **Capacidade provisionada**: Um sistema de arquivos (volume) que foi alocado de um sistema Cloud Volumes ONTAP e está pronto para armazenar dados de usuário ou aplicativo.
- **Reservado**: A quantidade de espaço reservado para volumes já provisionados em um nível local.
- **Usado**: A quantidade de espaço que contém dados.
- **Usado e reservado**: A soma do espaço físico utilizado e reservado.

Capacidade de uma VM de storage

A capacidade máxima de uma VM de armazenamento é determinada pelo espaço total alocado para volumes mais o espaço não alocado restante.

- O espaço alocado para volumes é a soma da capacidade usada e a soma da capacidade disponível dos volumes FlexVol, volumes FlexGroup e volumes FlexCache.
- A capacidade dos volumes está incluída nas somas, mesmo quando elas estão restritas, offline ou na fila de recuperação após a exclusão.
- Se os volumes estiverem configurados com crescimento automático, o valor máximo de dimensionamento automático do volume será usado nas somas. Sem crescimento automático, a capacidade real do volume é usada nas somas.

O gráfico a seguir explica como a medição da capacidade entre volumes se relaciona com o limite máximo de capacidade.



A partir do ONTAP 9.13,1, os administradores de cluster podem "Habilite um limite máximo de capacidade para uma VM de storage". No entanto, os limites de storage não podem ser definidos para uma VM de storage que contenha volumes para proteção de dados, em um relacionamento com a SnapMirror ou em uma

configuração do MetroCluster. Além disso, as cotas não podem ser configuradas para exceder a capacidade máxima de uma VM de armazenamento.

Depois de definir o limite máximo de capacidade, não pode ser alterado para um tamanho inferior à capacidade atualmente alocada.

Quando uma VM de armazenamento atinge seu limite máximo de capacidade, certas operações não podem ser executadas. O System Manager fornece sugestões para as próximas etapas no **"Insights"**.

Unidades de medição da capacidade

O System Manager calcula a capacidade de armazenamento com base em unidades binárias de 1024 (2,10) bytes.

- A partir do ONTAP 9.10,1, as unidades de capacidade de armazenamento são exibidas no System Manager como KiB, MIB, GiB, TIB e PIB.
- No ONTAP 9.10,0 e anterior, essas unidades são exibidas no Gerenciador de sistema como KB, MB, GB, TB e PB.

As unidades usadas no Gerenciador de sistemas para taxa de transferência continuam a ser KB/s, MB/s, GB/s, TB/s e PB/s para todas as versões do ONTAP.

Unidade de capacidade exibida no Gerenciador do sistema para ONTAP 9.10,0 e anterior	Unidade de capacidade exibida no Gerenciador do sistema para ONTAP 9.10,1 e posterior	Cálculo	Valor em bytes
KB	KiB	1024	1024 bytes
MB	MIB	1024 * 1024	1.048.576 bytes
GB	Gib	1024 * 1024 * 1024	1.073.741.824 bytes
TB	TIB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes
PB	PIB	1024 * 1024 * 1024 * 1024 * 1024	1.125.899.906.842.624 bytes

Informações relacionadas

"Monitorar a capacidade no System Manager"

"Relatórios de espaço lógico e imposição para volumes"

Gerenciamento de storage lógico com a CLI

Visão geral do gerenciamento lógico de storage com a CLI

Com a CLI do ONTAP, você pode criar e gerenciar volumes do FlexVol, usar a tecnologia

FlexClone para criar cópias eficientes de volumes, arquivos e LUNs, criar qtrees e cotas, além de gerenciar recursos de eficiência, como deduplicação e compactação.

Você deve usar esses procedimentos nas seguintes circunstâncias:

- Você quer entender a variedade de funcionalidades do ONTAP FlexVol volume e recursos de eficiência de storage.
- Você deseja usar a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Criar e gerenciar volumes

Crie um volume

Você pode criar um volume e especificar seu ponto de junção e outras propriedades usando o `volume create` comando.

Sobre esta tarefa

Um volume deve incluir um *caminho de junção* para que seus dados sejam disponibilizados aos clientes. Você pode especificar o caminho de junção ao criar um novo volume. Se você criar um volume sem especificar um caminho de junção, será necessário *montar* o volume no namespace SVM usando o `volume mount` comando.

Antes de começar

- O SVM para o novo volume e o agregado que fornecerá o storage ao volume já devem existir.
- Se o SVM tiver uma lista de agregados associados, o agregado precisará ser incluído na lista.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Criar um volume:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   As `-security style` opções , `-user`, `-group`, `-junction-path` e `-policy` são apenas para namespaces nas.

   As opções para `-junction-path` são as seguintes:

   - Diretamente sob a raiz, por exemplo, `/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado diretamente no volume raiz da SVM.

- Em um diretório existente, por exemplo, `/existing_dir/new_vol`

  Você pode criar um novo volume e especificar que ele seja montado em um volume existente (em uma hierarquia existente), expresso como um diretório.

Se você quiser criar um volume em um novo diretório (em uma nova hierarquia em um novo volume), por exemplo, `/new_dir/new_vol` será necessário criar primeiro um novo volume pai que seja juntado ao volume raiz SVM. Em seguida, você criaria o novo volume filho no caminho de junção do novo volume pai (novo diretório).

2. Verifique se o volume foi criado com o ponto de junção desejado:

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Exemplos

O comando a seguir cria um novo volume chamado users1 no SVM `vs1.example.com` e no agregado `aggr1`. O novo volume é disponibilizado em `/users`. O volume tem 750 GB de tamanho e sua garantia de volume é do tipo volume (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

O comando a seguir cria um novo volume chamado "'home4" na SVM"'vs1.example.com`'" e o agregado "'aggr1". O diretório `/eng/` já existe no namespace para o VS1 SVM, e o novo volume é disponibilizado no `/eng/home`, que se torna o diretório home do `/eng/` namespace. O volume é de 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- -------  -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Ative o suporte a grandes volumes e arquivos grandes no ONTAP

A partir do ONTAP 9.12.1 P2, você pode criar um novo volume ou modificar um volume

existente para habilitar o suporte para um tamanho máximo de volume de 300TB TB, "Volume FlexGroup"tamanho máximo de 60PB TB e tamanho máximo de arquivo (LUN) de 128TB TB.

Antes de começar

- O ONTAP 9.12,1 P2 ou posterior está instalado no cluster.
- Se você estiver habilitando o suporte de grande volume no cluster de origem em uma relação do SnapMirror, você deve ter o ONTAP 9.12,1 P2 ou posterior instalado no cluster que hospeda o volume de origem, bem como o cluster que hospeda o volume de destino.
- Você é um administrador de cluster ou SVM.
- Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Crie um novo volume

Passo

1. Crie um volume com suporte de arquivos e volume grande habilitado:

```
volume create -vserver <svm_name> -volume <volume_name> -aggregate
<aggregate_name> -is-large-size-enabled true
```

Exemplo

O exemplo a seguir cria um novo volume com suporte de grande volume e tamanho de arquivo ativado.

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large
-size-enabled true
```

Modificar um volume existente

Passo

1. Modifique um volume para permitir o suporte a grandes volumes e arquivos:

```
volume modify -vserver <svm_name> -volume <volume_name> -is-large-size
-enabled true
```

Exemplo

O exemplo a seguir modifica um volume existente para suportar grande volume e tamanho de arquivo.

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

2. Ative as novas definições de configuração remontando o volume:

```
volume unmount -vserver <svm_name> -volume <volume_name>
```

```
volume mount -vserver <svm_name> -volume <volume_name>
```

Informações relacionadas

- "Crie um volume"
- "Referência do comando"

Volumes SAN

Visão geral do provisionamento de volume SAN

O ONTAP fornece várias opções básicas para o provisionamento de volume de SAN. Cada opção usa um método diferente para gerenciar os requisitos de espaço de volume e espaço para as tecnologias de compartilhamento de blocos do ONTAP. Você deve entender como cada opção de provisionamento funciona para que você possa escolher a melhor opção para o seu ambiente.

Não é recomendável colocar LUNs SAN e compartilhamentos nas no mesmo FlexVol volume. Em vez disso, você deve provisionar volumes FlexVol separados para seus LUNs SAN e compartilhamentos nas. Isso simplifica as implantações de gerenciamento e replicação. Ele também é paralelo à maneira como os volumes do FlexVol são suportados no Active IQ Unified Manager (anteriormente OnCommand Unified Manager).

Thin Provisioning para volumes

Quando um volume provisionado é criado, o ONTAP não reserva nenhum espaço extra quando o volume é criado. À medida que os dados são gravados no volume, o volume solicita o storage de que ele precisa do agregado para acomodar a operação de gravação. O uso de volumes provisionados por thin permite comprometer seu agregado, o que introduz a possibilidade de o volume não ser capaz de proteger o espaço necessário quando o agregado ficar sem espaço livre.

Você cria um FlexVol volume com provisionamento reduzido definindo sua `-space-guarantee` opção como `none`.

Provisionamento espesso para volumes

Quando um volume provisionado com espessura é criado, o ONTAP reserva armazenamento suficiente do agregado para garantir que qualquer bloco no volume possa ser gravado a qualquer momento. Ao configurar um volume para usar o provisionamento thick, você pode empregar qualquer um dos recursos de eficiência de storage da ONTAP, como compactação e deduplicação, para compensar os maiores requisitos de storage iniciais.

Você cria um FlexVol volume com provisionamento excessivo definindo sua `-space-slo` opção (objetivo de nível de serviço) como `thick`.

Provisionamento semi-espesso para volumes

Quando um volume usando provisionamento semi-espesso é criado, o ONTAP separa o espaço de armazenamento do agregado para contabilizar o tamanho do volume. Se o volume estiver sem espaço livre porque os blocos estão em uso por tecnologias de compartilhamento de bloco, o ONTAP se esforça para

excluir objetos de dados de proteção (cópias Snapshot e arquivos FlexClone e LUNs) para liberar o espaço que eles estão segurando. Enquanto o ONTAP puder excluir os objetos de dados de proteção com a rapidez suficiente para acompanhar o espaço necessário para sobrescritas, as operações de gravação continuarão a ser bem-sucedidas. Isso é chamado de garantia de escrita "melhor esforço".

Não é possível empregar tecnologias de eficiência de storage, como deduplicação, compressão e compactação em um volume que esteja usando o provisionamento de meia espessura.

Você cria um FlexVol volume provisionado semi-espesso definindo sua `-space-slo` opção (objetivo de nível de serviço) como `semi-thick`.

Use com arquivos e LUNs reservados ao espaço

Um arquivo ou LUN com espaço reservado é aquele para o qual o armazenamento é alocado quando é criado. Historicamente, o NetApp usou o termo "LUN com provisionamento reduzido" para significar um LUN para o qual a reserva de espaço está desativada (um LUN sem espaço reservado).

Arquivos não reservados ao espaço geralmente não são chamados de "arquivos thin-provisionados".

A tabela a seguir resume as principais diferenças em como as três opções de provisionamento de volume podem ser usadas com arquivos reservados ao espaço e LUNs:

Provisionamento de volume	Reserva de espaço LUN/ficheiro	Sobrescreve	Proteção de dados 2	A eficiência de armazenamento 3
Espesso	Suportado	1	Garantido	Suportado
Fino	Sem efeito	Nenhum	Garantido	Suportado
Semi-espesso	Suportado	O melhor esforço 1	Melhor esforço	Não suportado

Notas

1. A capacidade de garantir substituições ou fornecer uma garantia de substituição de melhor esforço requer que a reserva de espaço esteja ativada no LUN ou arquivo.
2. Os dados de proteção incluem cópias Snapshot e arquivos FlexClone e LUNs marcados para exclusão automática (clones de backup).
3. A eficiência de storage inclui deduplicação, compactação, arquivos FlexClone e LUNs não marcados para exclusão automática (clones ativos) e subarquivos FlexClone (usados para descarregar cópias).

Suporte para LUNs de thin Provisioning SCSI

O ONTAP oferece suporte a T10 LUNs de thin Provisioning SCSI, bem como LUNs de thin Provisioning NetApp. O thin Provisioning SCSI T10 permite que os aplicativos host suportem recursos SCSI, incluindo recuperação de espaço LUN e recursos de monitoramento de espaço LUN para ambientes de blocos. O thin Provisioning SCSI T10 deve ser suportado pelo software de host SCSI.

Você usa a configuração ONTAP `space-allocation` para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 em um LUN. Você usa a configuração ONTAP `space-allocation enable` para habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

O `[-space-allocation {enabled|disabled}]` comando no Manual de Referência de comando do ONTAP tem mais informações para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 e habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

Informações relacionadas

- "Referência do comando ONTAP"

Configurar opções de provisionamento de volume

Você pode configurar um volume para thin Provisioning, provisionamento thick ou provisionamento semi-thick, dependendo dos requisitos de espaço.

Sobre esta tarefa

Definir a `-space-slo` opção para `thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- 100% do espaço necessário para as substituições é reservado. Você não pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`

Definir a `-space-slo` opção para `semi-thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- Nenhum espaço é reservado para substituições. Você pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`.
- A exclusão automática de cópias Snapshot está ativada.

Passo

1. Configurar opções de provisionamento de volume:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   A `-space-guarantee` opção padrão é `none` para sistemas AFF e para volumes DP não AFF. Caso contrário, o padrão é `volume`. Para volumes FlexVol existentes, use o `volume modify` comando para configurar opções de provisionamento.

   O comando a seguir configura o vol1 no SVM VS1 para thin Provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   O comando a seguir configura o vol1 no SVM VS1 para provisionamento espesso:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento semi-espesso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
thick
```

Determinar o uso de espaço em um volume ou agregado

Em alguns casos, ativar um recurso no ONTAP pode consumir mais espaço do que o esperado. O ONTAP ajuda você a determinar como o espaço está sendo consumido fornecendo três perspetivas para visualizar o espaço: O volume, a pegada de um volume dentro do agregado e o agregado.

Ver alocação de espaço

Um volume pode ficar sem espaço devido ao consumo de espaço ou espaço insuficiente dentro do volume, agregado ou uma combinação de ambos. Ao ver uma divisão orientada a recursos do uso do espaço de diferentes perspetivas, você pode avaliar quais recursos você pode querer ajustar ou desativar, ou se você deve tomar outra ação (como aumentar o tamanho do agregado ou do volume).

Você pode visualizar detalhes de uso do espaço a partir de qualquer uma dessas perspetivas:

- A utilização do espaço do volume

  Essa perspetiva fornece detalhes sobre o uso de espaço dentro do volume, incluindo o uso de cópias Snapshot.

  Use o `volume show-space` comando para ver o uso de espaço de um volume.

  A partir do ONTAP 9.14,1, em volumes com Eficiência de armazenamento sensível à temperatura (TSSE) habilitado, a quantidade de espaço usado no volume relatado pelo `volume show-space -physical used` comando inclui a economia de espaço obtida como resultado do TSSE.

- A pegada do volume dentro do agregado

  Essa perspetiva fornece detalhes sobre a quantidade de espaço que cada volume está usando no agregado contendo, incluindo os metadados do volume.

  Use o `volume show-footprint` comando para ver a pegada de um volume com o agregado.

- O uso de espaço do agregado

  Essa perspectiva inclui totais de pegadas de volume de todos os volumes contidos no agregado, espaço reservado para cópias Snapshot agregadas e outros metadados agregados.

  O WAFL reserva 10% do espaço total em disco para metadados de nível agregado e performance. O espaço usado para manter os volumes no agregado sai da reserva WAFL e não pode ser alterado.

  A partir do ONTAP 9.12,1, a reserva WAFL para agregados maiores que 30TB é reduzida de 10% para 5% para plataformas AFF e para plataformas FAS500f. A partir do ONTAP 9.14,1, essa mesma redução se aplica a agregados em todas as plataformas FAS, resultando em 5% mais espaço utilizável nos agregados.

Use o `storage aggregate show-space` comando para ver o uso do espaço do agregado.

Certos recursos, como backup em fita e deduplicação, usam espaço para metadados do volume e diretamente do agregado. Esses recursos mostram o uso de espaço diferente entre as perspetivas de volume e volume.

Informações relacionadas

- "artigo da base de conhecimento: Uso do espaço"
- "Libere até 5% da sua capacidade de armazenamento atualizando para o ONTAP 9.12,1"

Relatórios de metadados de volume e métricas de dados

Historicamente, várias das métricas de espaço de volume relataram o total de dados consumidos como uma combinação de duas métricas: Metadados e dados do usuário. A partir do ONTAP 9.15,1, os metadados e as métricas de dados do usuário são relatados separadamente. Dois novos contadores de metadados foram introduzidos para dar suporte a isso:

- metadados totais

  Este contador fornece o tamanho total dos metadados dentro do volume. Ele não inclui os metadados de volume residente agregado. Relatá-lo separadamente ajuda a determinar os dados lógicos alocados pelo usuário.

- espaço físico total dos metadados

  Este contador é a soma dos metadados residentes em volume e dos metadados de volume residente agregados. Ele fornece o espaço total dos metadados do volume dentro do agregado. Relatá-lo separadamente ajuda a determinar os dados físicos alocados pelo usuário.

Além disso, vários contadores existentes foram atualizados para remover o componente de metadados e apresentar apenas os dados do usuário:

- Dados do utilizador
- Espaço físico dos dados do volume

Essas alterações fornecem uma visão mais precisa dos dados consumidos pelo usuário. Isso tem vários benefícios, incluindo a capacidade de tomar decisões de chargeback mais precisas.

Ative a eliminação automática de instantâneos e LUN para gerir o espaço

Você pode definir e ativar uma política para excluir automaticamente snapshots e LUNs FlexClone. A exclusão automática de snapshots e LUNs do FlexClone ajuda você a gerenciar a utilização do espaço.

Sobre esta tarefa

É possível excluir automaticamente snapshots de volumes de leitura/gravação e LUNs do FlexClone de volumes pai de leitura/gravação. Não é possível configurar a exclusão automática de instantâneos de volumes somente leitura, por exemplo, volumes de destino do SnapMirror.

Passo

1. Defina e ative uma política para eliminar automaticamente instantâneos utilizando o `volume snapshot autodelete modify` comando.

Consulte a `volume snapshot autodelete modify` página de manual para obter informações sobre os parâmetros que você pode usar com este comando para definir uma política que atenda às suas necessidades.

O comando a seguir habilita a exclusão automática de snapshots e define o gatilho para `snap_reserve` o volume vol3, que faz parte da máquina virtual de armazenamento vs0.example.com (SVM):

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger snap_reserve
```

O comando a seguir permite a exclusão automática de snapshots e LUNs FlexClone marcados para exclusão automática para o volume vol3, que faz parte da máquina virtual de storage vs0.example.com (SVM):

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```

Os snapshots em nível agregado funcionam de forma diferente dos snapshots em nível de volume e são gerenciados automaticamente pelo ONTAP. A opção de excluir snapshots agregados está sempre ativada e ajuda a gerenciar a utilização de espaço.

Se o parâmetro trigger for definido como `snap_reserve` para um agregado, os instantâneos serão mantidos até que o espaço reservado cruze a capacidade limite. Portanto, mesmo que o parâmetro trigger não esteja definido como `snap_reserve`, o espaço usado pela cópia snapshot no comando será listado como `0` porque esses snapshots são excluídos automaticamente. Além disso, o espaço usado por snapshots em um agregado é considerado livre e está incluído no parâmetro espaço disponível do comando.

Configure os volumes para fornecer automaticamente mais espaço quando estiverem cheios

Quando o FlexVol volumes ficar cheio, o ONTAP pode usar vários métodos para tentar fornecer automaticamente mais espaço livre para o volume. Você escolhe quais métodos o ONTAP pode usar e em que ordem, dependendo dos requisitos impostos pela arquitetura de storage e aplicativo.

Sobre esta tarefa

O ONTAP pode fornecer automaticamente mais espaço livre para um volume completo usando um ou ambos os seguintes métodos:

- Aumente o tamanho do volume (conhecido como *crescimento automático*).

  Este método é útil se o volume contendo agregado tiver espaço suficiente para suportar um volume maior. Pode configurar o ONTAP para definir um tamanho máximo para o volume. O aumento é acionado automaticamente com base na quantidade de dados que estão sendo gravados no volume em relação à quantidade atual de espaço usado e quaisquer limites definidos.

O crescimento automático não é acionado para suportar a criação de cópias Snapshot. Se você tentar criar uma cópia Snapshot e não houver espaço suficiente, a criação da cópia Snapshot falhará, mesmo com o crescimento automático ativado.

- Exclua cópias Snapshot, arquivos FlexClone ou LUNs FlexClone.

  Por exemplo, você pode configurar o ONTAP para excluir automaticamente cópias Snapshot que não estão vinculadas a cópias Snapshot em volumes clonados ou LUNs, ou definir quais cópias snapshot deseja ONTAP excluir primeiro - suas cópias Snapshot mais antigas ou mais recentes. Você também pode determinar quando o ONTAP deve começar a excluir cópias snapshot - por exemplo, quando o volume está quase cheio ou quando a reserva de snapshot do volume está quase cheia.

Se você ativar ambos os métodos, poderá especificar qual método o ONTAP tenta primeiro quando um volume está quase cheio. Se o primeiro método não fornecer espaço adicional suficiente para o volume, o ONTAP tenta o outro método em seguida.

Por padrão, o ONTAP tenta aumentar primeiro o tamanho do volume. Na maioria dos casos, a configuração padrão é preferível, porque quando uma cópia Snapshot é excluída, ela não pode ser restaurada. No entanto, se você precisar evitar aumentar o tamanho de um volume sempre que possível, poderá configurar o ONTAP para excluir cópias Snapshot antes de aumentar o tamanho do volume.

Passos

1. Se você quiser que o ONTAP tente aumentar o tamanho do volume quando ele ficar cheio, ative a capacidade de crescimento automático para o volume usando o `volume autosize` comando com `grow` modo.

   Lembre-se de que quando o volume cresce, ele consome mais espaço livre de seu agregado associado. Se você estiver dependendo da capacidade do volume de crescer sempre que precisar, você deve monitorar o espaço livre no agregado associado e adicionar mais quando necessário.

2. Se você quiser que o ONTAP exclua cópias Snapshot, arquivos FlexClone ou LUNs FlexClone quando o volume ficar cheio, habilite o modo de operação para esses tipos de objetos.
3. Se você ativou o recurso de volume com crescimento automático e um ou mais recursos de transferência de dados, selecione o primeiro método que o ONTAP deve usar para fornecer espaço livre a um volume usando o `volume modify` comando com a `-space-mgmt-try-first` opção.

   Para especificar o aumento do tamanho do volume primeiro (o padrão), use `volume_grow`. Para especificar primeiro a exclusão de cópias Snapshot, use `snap_delete`o .

Configure volumes para aumentar e diminuir automaticamente o tamanho

Você pode configurar os volumes do FlexVol para aumentar e diminuir automaticamente de acordo com a quantidade de espaço que eles atualmente exigem. O crescimento automático ajuda a evitar que um volume fique sem espaço, se o agregado puder fornecer mais espaço. O encolhimento automático impede que um volume seja maior do que o necessário, liberando espaço no agregado para uso por outros volumes.

Sobre esta tarefa

O Autoshink só pode ser usado em combinação com o crescimento automático para atender às demandas de espaço em constante mudança e não está disponível sozinho. Quando a opção Autoshink está ativada, o ONTAP gerencia automaticamente o comportamento de encolhimento de um volume para evitar um ciclo infinito de ações com crescimento automático e com redução automática.

À medida que um volume aumenta, o número máximo de arquivos que ele pode conter pode ser aumentado automaticamente. Quando um volume é reduzido, o número máximo de arquivos que ele pode conter permanece inalterado e um volume não pode ser encolhido automaticamente abaixo do tamanho que corresponde ao número máximo de arquivos atual. Por esse motivo, pode não ser possível reduzir automaticamente um volume até o tamanho original.

Por padrão, o tamanho máximo para o qual um volume pode crescer é de 120% do tamanho no qual o crescimento automático é ativado. Se você precisar garantir que o volume pode crescer para ser maior do que isso, você deve definir o tamanho máximo para o volume de acordo.

Antes de começar

O FlexVol volume deve estar online.

Passo

1. Configure o volume para crescer e diminuir seu tamanho automaticamente:

   `volume autosize -vserver` *`SVM_name`* `-volume` *`volume_name`* `-mode grow_shrink`

   O comando a seguir habilita alterações automáticas de tamanho para um volume chamado test2. O volume é configurado para começar a diminuir quando está 60% cheio. Os valores padrão são usados para quando começará a crescer e seu tamanho máximo.

   ```
   cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
   60
   vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

   Volume modify successful on volume: test2
   ```

Requisitos para habilitar a exclusão automática de cópia Snapshot e automática

A funcionalidade de redução automática pode ser usada com a exclusão automática de cópia Snapshot, desde que certos requisitos de configuração sejam atendidos.

Se você quiser habilitar a funcionalidade de redução automática e a exclusão automática de cópia Snapshot, sua configuração deverá atender aos seguintes requisitos:

- O ONTAP deve ser configurado para tentar aumentar o tamanho do volume antes de tentar excluir cópias snapshot (a `-space-mgmt-try-first` opção deve ser definida como `volume_grow`).
- O gatilho para a exclusão automática de cópia Snapshot deve ser volume (o `trigger` parâmetro deve ser definido como `volume`).

Funcionalidade de redução automática e eliminação de cópia instantânea

Como a funcionalidade de redução automática diminui o tamanho de um FlexVol volume, ele também pode afetar quando as cópias snapshot de volume são excluídas automaticamente.

A funcionalidade de redução automática interage com a exclusão automática de cópia Snapshot do volume das seguintes maneiras:

- Se o `grow_shrink` modo automático e a exclusão automática de cópia Snapshot estiverem ativados, quando um tamanho de volume diminuir, ele poderá acionar uma exclusão automática de cópia Snapshot.

  Isso ocorre porque a reserva Snapshot é baseada em uma porcentagem do tamanho do volume (5% por padrão), e essa porcentagem agora é baseada em um tamanho de volume menor. Isso pode fazer com que cópias Snapshot saiam da reserva e sejam excluídas automaticamente.

- Se o `grow_shrink` modo de dimensionamento automático estiver ativado e você excluir manualmente uma cópia Snapshot, ela poderá acionar um encolhimento automático de volume.

Address FlexVol volume fullness e alertas de sobrealocação

O ONTAP emite mensagens do EMS quando os volumes do FlexVol estão ficando sem espaço para que você possa tomar medidas corretivas fornecendo mais espaço para o volume total. Conhecer os tipos de alertas e como abordá-los ajuda a garantir a disponibilidade dos dados.

Quando um volume é descrito como *full*, significa que a porcentagem do espaço no volume disponível para uso pelo sistema de arquivos ativo (dados do usuário) caiu abaixo de um limite (configurável). Quando um volume se torna *superalocado*, o espaço usado pelo ONTAP para metadados e para suportar o acesso básico a dados foi esgotado. Às vezes, o espaço normalmente reservado para outros fins pode ser usado para manter o volume funcionando, mas a reserva de espaço ou a disponibilidade de dados podem estar em risco.

A sobrealocação pode ser lógica ou física. *Sobrealocação lógica* significa que o espaço reservado para honrar compromissos futuros de espaço, como reserva de espaço, foi usado para outro propósito. *Superalocação física* significa que o volume está ficando sem blocos físicos para usar. Os volumes nesse estado correm o risco de recusar gravações, ficar offline ou potencialmente causar uma interrupção do controlador.

Um volume pode estar mais de 100% cheio devido ao espaço usado ou reservado pelos metadados. No entanto, um volume que seja superior a 100% completo pode ou não ser superalocado. Se houver compartilhamentos no nível de qtree e no nível de volume no mesmo pool FlexVol ou SCVMM, os qtrees aparecerão como diretórios no compartilhamento FlexVol. Portanto, você precisa ter cuidado para não excluí-los acidentalmente.

A tabela a seguir descreve os alertas de volume e sobrealocação, as ações que você pode tomar para resolver o problema e os riscos de não tomar medidas:

Tipo de alerta	Nível EMS	Configurável?	Definição	Formas de abordar	Risco se nenhuma ação for tomada
Quase cheio	Depurar	Y	O sistema de arquivos excedeu o limite definido para esse alerta (o padrão é 95%). A porcentagem é o `Used` total menos o tamanho da reserva Snapshot.	• Aumentar o tamanho do volume • Redução dos dados do usuário	Não há risco de gravar operações ou disponibilidade de dados ainda.

Tipo de alerta	Nível EMS	Configurável?	Definição	Formas de abordar	Risco se nenhuma ação for tomada
Cheio	Depurar	Y	O sistema de arquivos excedeu o limite definido para esse alerta (o padrão é 98%). A porcentagem é o `Used` total menos o tamanho da reserva Snapshot.	• Aumentar o tamanho do volume • Redução dos dados do usuário	Não há risco de gravar operações ou disponibilidade de dados ainda, mas o volume está se aproximando do estágio em que as operações de gravação podem estar em risco.
Logicamente sobralocada	Erro SVC	N	Além de o sistema de arquivos estar cheio, o espaço no volume usado para metadados foi esgotado.	• Aumentar o tamanho do volume • Exclusão de cópias Snapshot • Redução dos dados do usuário • Desativar reserva de espaço para ficheiros ou LUNs	As operações de gravação em arquivos não reservados podem falhar.
Fisicamente sobrealocado	Erro nó	N	O volume está ficando sem blocos físicos nos quais pode escrever.	• Aumentar o tamanho do volume • Exclusão de cópias Snapshot • Redução dos dados do usuário	As operações de gravação estão em risco, bem como a disponibilidade de dados; o volume pode ficar offline.

Sempre que um limite é cruzado para um volume, quer a percentagem de plenitude esteja a aumentar ou a cair, é gerada uma mensagem EMS. Quando o nível de plenitude do volume cai abaixo de um limite, uma `volume ok` mensagem EMS é gerada.

Endereça alertas de preenchimento agregado e sobrealocação

O ONTAP emite mensagens EMS quando os agregados estão ficando sem espaço para que você possa tomar medidas corretivas fornecendo mais espaço para o agregado

total. Conhecer os tipos de alertas e como resolvê-los ajuda a garantir a disponibilidade dos dados.

Quando um agregado é descrito como *full*, significa que a porcentagem do espaço no agregado disponível para uso por volumes caiu abaixo de um limite predefinido. Quando um agregado se torna *superalocado*, o espaço usado pelo ONTAP para metadados e para suportar o acesso básico a dados foi esgotado. Às vezes, o espaço normalmente reservado para outros fins pode ser usado para manter o funcionamento agregado, mas as garantias de volume para volumes associados com o agregado ou a disponibilidade de dados podem estar em risco.

A sobrealocação pode ser lógica ou física. *Sobrealocação lógica* significa que o espaço reservado para honrar futuros compromissos espaciais, como garantias de volume, foi usado para outro propósito. *Superalocação física* significa que o agregado está ficando sem blocos físicos para usar. Os agregados nesse estado correm o risco de recusar gravações, ficar offline ou potencialmente causar interrupção de uma controladora.

A tabela a seguir descreve os alertas de preenchimento agregado e sobrealocação, as ações que você pode tomar para resolver o problema e os riscos de não tomar medidas.

Tipo de alerta	Nível EMS	Configurável?	Definição	Formas de abordar	Risco se nenhuma ação for tomada
Quase cheio	Depurar	N	A quantidade de espaço atribuído aos volumes, incluindo as suas garantias, excedeu o limiar fixado para este alerta (95%). A porcentagem é o `Used` total menos o tamanho da reserva Snapshot.	• Adicionando armazenamento ao agregado • Redução ou exclusão de volumes • Mover volumes para outro agregado com mais espaço • Remoção das garantias de volume (definindo-as para `none`)	Não há risco de gravar operações ou disponibilidade de dados ainda.
Cheio	Depurar	N	O sistema de ficheiros excedeu o limite definido para este alerta (98%). A porcentagem é o `Used` total menos o tamanho da reserva Snapshot.	• Adicionando armazenamento ao agregado • Redução ou exclusão de volumes • Mover volumes para outro agregado com mais espaço • Remoção das garantias de volume (definindo-as para `none`)	As garantias de volume para volumes no agregado podem estar em risco, bem como as operações de gravação nesses volumes.

Tipo de alerta	Nível EMS	Configurável?	Definição	Formas de abordar	Risco se nenhuma ação for tomada
Logicamente sobralocada	Erro SVC	N	Além do espaço reservado para os volumes estarem cheios, o espaço no agregado usado para metadados foi esgotado.	• Adicionando armazenamento ao agregado • Redução ou exclusão de volumes • Mover volumes para outro agregado com mais espaço • Remoção das garantias de volume (definindo-as para `none`)	As garantias de volume para volumes no agregado estão em risco, bem como as operações de gravação nesses volumes.
Fisicamente sobrealocado	Erro nó	N	O agregado está ficando sem blocos físicos nos quais pode escrever.	• Adicionando armazenamento ao agregado • Redução ou exclusão de volumes • Mover volumes para outro agregado com mais espaço	As operações de gravação em volumes no agregado estão em risco, bem como a disponibilidade de dados; o agregado pode ficar offline. Em casos extremos, o nó pode sofrer uma interrupção.

Toda vez que um limite é cruzado para um agregado, quer a porcentagem de plenitude esteja aumentando ou caindo, uma mensagem EMS é gerada. Quando o nível de plenitude do agregado cai abaixo de um limite, uma `aggregate ok` mensagem EMS é gerada.

Considerações ao definir a reserva fracionária

A reserva fracionária, também chamada de *reserva de substituição LUN*, permite desativar a reserva de substituição para LUNs e arquivos reservados no espaço em um FlexVol volume. Isso pode ajudar você a maximizar a utilização do storage.

Se o seu ambiente for afetado negativamente pelas falhas nas operações de gravação devido à falta de espaço, você precisa entender os requisitos que essa configuração pode impor.

A configuração de reserva fracionária é expressa como uma porcentagem; os únicos valores válidos são `0` e `100` porcentagem. A configuração de reserva fracionária é um atributo do volume. Definir a reserva fracionária para `0` aumentar a utilização do armazenamento. No entanto, um aplicativo que acessa dados que residem no volume pode ter uma interrupção de dados se o volume estiver sem espaço livre, mesmo com a garantia de volume definida como `volume`. No entanto, com a configuração e o uso adequados de volume, você pode minimizar a chance de falhas de gravação. O ONTAP fornece uma garantia de gravação "melhor esforço" para volumes com reserva fracionária definida para `0` quando *todos* dos seguintes requisitos são atendidos:

- A deduplicação não está em uso
- A compressão não está a ser utilizada
- Os subficheiros FlexClone não estão a ser utilizados
- Todos os arquivos FlexClone e LUNs FlexClone são ativados para exclusão automática

  Esta não é a configuração padrão. Você deve ativar explicitamente a exclusão automática, seja no momento da criação ou modificando o arquivo FlexClone ou LUN FlexClone depois que ele for criado.
- A descarga de cópia ODX e FlexClone não está em uso
- A garantia de volume está definida para `volume`
- A reserva de espaço de arquivo ou LUN é `enabled`
- A reserva de instantâneo de volume está definida como `0`
- A exclusão automática da cópia Snapshot do volume é `enabled` com um nível de compromisso de `destroy`, uma lista de destruição de `lun_clone,vol_clone,cifs_share,file_clone,sfsr` e um gatilho de `volume`

  Essa configuração também garante que arquivos FlexClone e LUNs FlexClone sejam excluídos quando necessário.

- Se todos os requisitos acima forem atendidos, mas sua taxa de alteração for alta, em casos raros, a exclusão automática da cópia Snapshot pode ficar para trás, o que faz com que o volume fique sem espaço.
- Se todos os requisitos acima forem atendidos e as cópias Snapshot não estiverem em uso, as gravações de volume não ficarão sem espaço.

Além disso, você pode, como opção, usar a funcionalidade de volume com crescimento automático para diminuir a probabilidade de as cópias do Snapshot precisarem ser excluídas automaticamente. Se você ativar a capacidade de crescimento automático, deverá monitorar o espaço livre no agregado associado. Se o agregado ficar cheio o suficiente para que o volume seja impedido de crescer, mais cópias Snapshot provavelmente serão excluídas à medida que o espaço livre no volume estiver esgotado.

Se você não puder atender a todos os requisitos de configuração acima e precisar garantir que o volume não fique sem espaço, defina a configuração de reserva fracionária do volume como `100`. Isso requer mais espaço livre na frente, mas garante que as operações de modificação de dados serão bem-sucedidas mesmo quando as tecnologias listadas acima estiverem em uso.

O valor padrão e os valores permitidos para a configuração de reserva fracionária dependem da garantia do volume:

Garantia de volume	Reserva fracionária predefinida	Valores permitidos
Volume	100	0, 100
Nenhum	0	0, 100

Determine o uso de arquivos e inode para um volume

Os volumes FlexVol têm um número máximo de arquivos que podem conter. Você pode

usar um comando CLI para determinar se você precisa aumentar o número de inodes (públicos) para seus volumes FlexVol para evitar que eles atinjam seu limite de arquivos.

Sobre esta tarefa

Inodes públicos podem ser livres (não estão associados a um arquivo) ou usados (apontam para um arquivo). O número de inodes livres para um volume é o número total de inodes para o volume menos o número de inodes usados (o número de arquivos).

Se houver compartilhamentos no nível de qtree e no nível de volume no mesmo pool FlexVol ou SCVMM, os qtrees aparecerão como diretórios no compartilhamento FlexVol. Portanto, você precisa ter cuidado para não excluí-los acidentalmente.

Passos

1. Para exibir o uso de inode para um volume, digite o seguinte comando:

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files
```

Exemplo

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files
Vserver Name: vs1
Files Used (for user-visible data): 98
```

Controle e monitore o desempenho de e/S do FlexVol volume com a QoS de storage

Você pode controlar a performance de entrada/saída (e/S) a volumes FlexVol atribuindo volumes a grupos de políticas QoS de storage. Você pode controlar a performance de e/S para garantir que os workloads atinjam objetivos de performance específicos ou para controlar um workload que afeta negativamente outros workloads.

Sobre esta tarefa

Os grupos de políticas aplicam um limite máximo de taxa de transferência (por exemplo, 100 MB/s). Você pode criar um grupo de políticas sem especificar uma taxa de transferência máxima, que permite monitorar o desempenho antes de controlar a carga de trabalho.

Também é possível atribuir SVMs, LUNs e arquivos a grupos de políticas.

Observe os seguintes requisitos sobre a atribuição de um volume a um grupo de políticas:

- O volume deve estar contido pelo SVM ao qual o grupo de políticas pertence.

  Você especifica o SVM ao criar o grupo de políticas.

- Se você atribuir um volume a um grupo de políticas, não poderá atribuir o volume que contém SVM ou LUNs ou arquivos filhos a um grupo de políticas.

Para obter mais informações sobre como usar QoS de armazenamento, consulte "Referência de administração do sistema".

Passos

1. Use o `qos policy-group create` comando para criar um grupo de políticas.
2. Use o `volume create` comando ou o `volume modify` comando com o `-qos-policy-group` parâmetro para atribuir um volume a um grupo de políticas.
3. Use os `qos statistics` comandos para exibir dados de desempenho.
4. Se necessário, use o `qos policy-group modify` comando para ajustar o limite máximo de taxa de transferência do grupo de políticas.

Eliminar um FlexVol volume

Você pode excluir um FlexVol volume que não seja mais necessário.

O que você vai precisar

Nenhum aplicativo deve estar acessando os dados no volume que deseja excluir.

Se eliminar acidentalmente um volume, consulte o artigo da base de dados de Conhecimento "Como utilizar a fila de recuperação de volume".

Passos

1. Se o volume tiver sido montado, desmonte-o:

   ```
   volume unmount -vserver vserver_name -volume volume_name
   ```

2. Se o volume for parte de uma relação SnapMirror, exclua a relação usando o `snapmirror delete` comando.
3. Se o volume estiver online, coloque o volume offline:

   ```
   volume offline -vserver vserver_name volume_name
   ```

4. Eliminar o volume:

   ```
   volume delete -vserver vserver_name volume_name
   ```

Resultado

O volume é excluído, juntamente com quaisquer políticas de cota associadas e qtrees.

Proteção contra a exclusão acidental de volume

O comportamento de exclusão de volume padrão ajuda a recuperação de volumes FlexVol excluídos acidentalmente.

```
`volume delete`Uma solicitação contra um volume que tenha tipo `RW` ou
`DP` (como visto na `volume show` saída de comando) faz com que esse
volume seja movido para um estado parcialmente excluído. Por padrão, ele é
mantido em uma fila de recuperação por pelo menos 12 horas antes de ser
totalmente excluído.
```

Para obter mais informações, consulte o artigo da base de conhecimento "Como utilizar a fila de recuperação de volume".

Comandos para gerenciar volumes do FlexVol

A CLI do ONTAP fornece comandos específicos para o gerenciamento de volumes do FlexVol. Dependendo do que você precisa fazer, você pode usar os seguintes comandos para gerenciar volumes do FlexVol:

Se você quiser…	Use este comando…
Coloque um volume online	`volume online`
Altere o tamanho de um volume	`volume size`
Determine o agregado associado de um volume	`volume show`
Determinar o agregado associado para todos os volumes em uma máquina virtual de storage (SVM)	`volume show -vserver -fields aggregate`
Determine o formato de um volume	`volume show -fields block-type`
Monte um volume em outro volume usando uma junção	`volume mount`
Coloque um volume no estado restrito	`volume restrict`
Renomeie um volume	`volume rename`
Tire um volume off-line	`volume offline`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para exibir informações de uso de espaço

Você usa `storage aggregate` os comandos e `volume` para ver como o espaço está sendo usado em agregados, volumes e cópias Snapshot delas.

Para exibir informações sobre…	Use este comando…
Agregados, incluindo detalhes sobre porcentagens de espaço usado e disponível, tamanho da reserva do Snapshot e outras informações de utilização de espaço	`storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`
Como discos e grupos RAID são usados em um agregado e status RAID	`storage aggregate show-status`

Para exibir informações sobre…	Use este comando…
A quantidade de espaço em disco que seria recuperada se você excluísse uma cópia Snapshot específica	`volume snapshot compute-reclaimable` (avançado)
A quantidade de espaço utilizada por um volume	`volume show -fields size,used,available,percent-used` `volume show-space`
A quantidade de espaço usada por um volume no agregado que contém	`volume show-footprint`

Mover e copiar volumes

Mover uma visão geral do FlexVol volume

Você pode mover ou copiar volumes para utilização de capacidade, performance aprimorada e atender a contratos de nível de serviço. Saber como funciona a movimentação de um FlexVol volume ajuda você a determinar se a movimentação de volume atende a contratos de nível de serviço e a entender onde uma movimentação de volume está no processo de movimentação de volume.

Os volumes do FlexVol são movidos de um agregado ou nó para outro na mesma máquina virtual de storage (SVM). Uma movimentação de volume não interrompe o acesso do cliente durante a movimentação.

> Durante a fase de transição de uma operação de movimentação de volume, não é possível criar arquivos FlexClone ou LUNs FlexClone de um FlexVol volume.

Mover um volume ocorre em várias fases:

- Um novo volume é feito no agregado de destino.
- Os dados do volume original são copiados para o novo volume.

  Durante esse tempo, o volume original está intacto e disponível para os clientes acessarem.

- No final do processo de mudança, o acesso ao cliente é bloqueado temporariamente.

  Durante esse tempo, o sistema executa uma replicação final do volume de origem para o volume de destino, troca as identidades dos volumes de origem e destino e altera o volume de destino para o volume de origem.

- Depois de concluir a mudança, o sistema encaminha o tráfego do cliente para o novo volume de origem e retoma o acesso do cliente.

A mudança não causa interrupções no acesso do cliente porque o tempo em que o acesso do cliente é bloqueado termina antes que os clientes notem uma interrupção e um tempo limite. O acesso do cliente está bloqueado por 35 segundos por padrão. Se a operação de movimentação de volume não puder terminar no momento em que o acesso é negado, o sistema aborta essa fase final da operação de movimentação de volume e permite o acesso do cliente. O sistema tenta a fase final três vezes por padrão. Após a terceira

tentativa, o sistema aguarda uma hora antes de tentar novamente a sequência de fase final. O sistema executa a fase final da operação de movimentação de volume até que a movimentação de volume esteja concluída.

Considerações e recomendações ao mover volumes

Há várias considerações e recomendações a serem observadas ao mover um volume. Estes são baseados no volume que você está movendo, bem como na configuração do sistema, como o MetroCluster. Você deve entender todos os problemas relevantes antes de mover um volume.

Considerações gerais e recomendações

- Se você estiver atualizando a família de versões de um cluster, não mova um volume até que você atualize todos os nós do cluster.

  Esta recomendação impede que você tente inadvertidamente mover um volume de uma família de versões mais recente para uma família de versões mais antiga.

- O volume de origem deve ser consistente.
- Se você tiver atribuído um ou mais agregados à máquina virtual de storage (SVM) associada, o agregado de destino deve ser um dos agregados atribuídos.
- Você não pode mover um volume de ou para um agregado de CFO adquirido.
- Se um volume que contém LUNs não estiver habilitado para NVFAIL antes de movê-lo, o volume será habilitado para NVFAIL após movê-lo.
- Você pode mover um volume de um agregado de Flash Pool para outro agregado de Flash Pool.
  - As políticas de armazenamento em cache desse volume também são movidas.
  - A movimentação pode afetar o desempenho do volume.
- É possível mover volumes entre um agregado de Flash Pool e um agregado que não seja Flash Pool.
  - Se você mover um volume de um agregado de pool flash para um agregado que não seja de pool flash, o ONTAP exibirá uma mensagem avisando que a movimentação pode afetar o desempenho do volume e perguntará se deseja continuar.
  - Se você mover um volume de um agregado que não seja Flash Pool para um agregado Flash Pool, o ONTAP atribuirá a `auto` política de armazenamento em cache.
- Os volumes têm as proteções de dados em repouso do agregado em que residem. Se você mover um volume de um agregado que consiste em unidades NSE para um que não o faça, o volume não terá mais proteção de dados em repouso do NSE.

Considerações e recomendações sobre o volume FlexClone

- Os volumes do FlexClone não podem estar offline quando estão sendo movidos.
- É possível mover volumes FlexClone de um agregado para outro agregado no mesmo nó ou em outro nó na mesma SVM sem iniciar o `vol clone split start` comando.

  Ao iniciar uma operação de movimentação de volume em um volume FlexClone, o volume do clone é dividido durante o processo de movimentação para um agregado diferente. Depois que a movimentação do volume no volume do clone estiver concluída, o volume que foi movido não aparece mais como um clone, mas aparece como um volume independente sem qualquer relação de clone com o volume pai anterior.

- As cópias Snapshot de volume do FlexClone não são perdidas após a migração de um clone.
- Você pode mover volumes pai do FlexClone de um agregado para outro agregado.

  Quando você move um volume pai do FlexClone, um volume temporário é deixado para trás que atua como um volume pai para todos os volumes do FlexClone. Não são permitidas operações no volume temporário, exceto para colocá-lo offline ou excluí-lo. Depois de todos os volumes FlexClone serem divididos ou destruídos, o volume temporário é limpo automaticamente.

- Depois de mover um volume filho do FlexClone, o volume não é mais um volume FlexClone.
- As operações do FlexClone Move são mutuamente exclusivas das operações de cópia ou divisão do FlexClone.
- Se uma operação de divisão de clones estiver em andamento, mover um volume pode falhar.

  Você não deve mover um volume até que as operações de divisão de clones estejam concluídas.

Considerações e recomendações do MetroCluster

- Durante uma movimentação de volume em uma configuração MetroCluster, quando um volume temporário é criado no agregado de destino no cluster de origem, um Registro do volume temporário correspondente ao volume no espelhado, mas não assimilado, agregado também é criado no cluster sobrevivente.
- Se ocorrer um switchover de MetroCluster antes da transição, o volume de destino tem um Registro e é um volume temporário (um volume do tipo TMP).

  Mover o trabalho reinicia no cluster sobrevivente (recuperação de desastres), relata uma falha e limpa todos os itens relacionados à movimentação, incluindo o volume temporário. Em qualquer caso em que a limpeza não possa ser feita corretamente, um EMS é gerado alertando o administrador do sistema para fazer a limpeza necessária.

- Se um switchover do MetroCluster ocorrer depois que a fase de transição tiver sido iniciada, mas antes que a tarefa de mudança tenha sido concluída (ou seja, a mudança atingiu um estágio em que ela pode atualizar o cluster para apontar para o agregado de destino), a tarefa de movimentação será reiniciada no cluster (recuperação de desastres) sobrevivente e será concluída.

  Todos os itens relacionados com o movimento são limpos, incluindo o volume temporário (fonte original). Em qualquer caso em que a limpeza não possa ser feita corretamente, um EMS é gerado alertando o administrador do sistema para fazer a limpeza necessária.

- Não são permitidos switchbacks MetroCluster forçados ou não forçados se houver operações de movimentação de volume em andamento para volumes pertencentes ao local comutado.

  Os switchbacks não são bloqueados quando as operações de movimentação de volume estão em andamento para volumes locais para o local sobrevivente.

- Os switchovers de MetroCluster não forçados são bloqueados, mas os switchovers de MetroCluster forçados não são bloqueados se houver operações de movimentação de volume em andamento.

Requisitos para movimentação de volumes em um ambiente SAN

Você precisa se preparar antes de mover um volume em um ambiente SAN.

Antes de mover um volume que contenha LUNs ou namespaces, você precisa atender aos seguintes requisitos:

- Para volumes que contêm um ou mais LUNs, você deve ter no mínimo dois caminhos por LUN (LIFs) conetados a cada nó no cluster.

  Isso elimina pontos únicos de falha e permite que o sistema sobreviva a falhas de componentes.

- Para volumes que contêm namespaces, o cluster precisa estar executando o ONTAP 9.6 ou posterior.

  A movimentação de volume não é compatível com configurações NVMe que executam o ONTAP 9.5.

Mover um volume

Você pode mover um FlexVol volume para um agregado, nó ou ambos diferentes na mesma máquina virtual de storage (SVM) para equilibrar a capacidade de storage depois de determinar que há um desequilíbrio de capacidade de storage.

Sobre esta tarefa

Por padrão, se a operação de transição não for concluída dentro de 30 segundos, ela tentará novamente. Você pode ajustar o comportamento padrão usando os `-cutover-window` parâmetros e `-cutover-action`, que exigem acesso avançado ao nível de privilégio. Para obter detalhes, consulte a `volume move start` página de manual.

Passos

1. Se você estiver movendo um espelho de proteção de dados e não tiver inicializado a relação de espelho, inicialize a relação de espelho usando o `snapmirror initialize` comando.

   As relações de espelho de proteção de dados devem ser inicializadas antes de poder mover um dos volumes.

2. Determine um agregado para o qual você pode mover o volume usando o `volume move target-aggr show` comando.

   O agregado que você selecionar deve ter espaço suficiente para o volume; ou seja, o tamanho disponível é maior do que o volume que você está movendo.

   O exemplo a seguir mostra que o volume VS2 pode ser movido para qualquer um dos agregados listados:

   ```
   cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
   Aggregate Name   Available Size   Storage Type
   --------------   --------------   ------------
   aggr2            467.9GB          hdd
   node12a_aggr3    10.34GB          hdd
   node12a_aggr2    10.36GB          hdd
   node12a_aggr1    10.36GB          hdd
   node12a_aggr4    10.36GB          hdd
   5 entries were displayed.
   ```

3. Verifique se o volume pode ser movido para o agregado pretendido usando o `volume move start -perform-validation-only` comando para executar uma verificação de validação.
4. Mova o volume usando o `volume move start` comando.

O comando a seguir move o volume user_Max no SVM VS2 para o agregado node12a_aggr3. O movimento é executado como um processo em segundo plano.

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

5. Determine o status da operação de movimentação de volume usando o `volume move show` comando.

   O exemplo a seguir mostra o estado de uma movimentação de volume que concluiu a fase de replicação e está na fase de transição:

```
cluster1::> volume move show
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       user_max   healthy  cutover     -                -
```

   A movimentação do volume está concluída quando não aparece mais na `volume move show` saída do comando.

Comandos para mover volumes

A CLI do ONTAP fornece comandos específicos para gerenciar a movimentação de volume. Dependendo do que você precisa fazer, use os seguintes comandos para gerenciar regras de cota e políticas de cota:

Se você quiser…	Use este comando…
Abortar uma operação de movimentação de volume ativa.	`volume move abort`
Mostrar o status de um volume que se move de um agregado para outro agregado.	`volume move show`
Comece a mover um volume de um agregado para outro agregado.	`volume move start`
Gerenciar agregados de destino para movimentação de volume.	`volume move target-aggr`
Acionar a transição de um trabalho de movimento.	`volume move trigger-cutover`

Se você quiser…	Use este comando…
Alterar a quantidade de tempo que o acesso do cliente é bloqueado se o padrão não for adequado.	`volume move start` ou `volume move modify` com o `-cutover-window` parâmetro. O `volume move modify` comando é um comando avançado e o `-cutover-window` é um parâmetro avançado.
Determine o que o sistema faz se a operação de movimentação de volume não puder ser concluída durante o tempo em que o acesso do cliente é bloqueado.	`volume move start` ou `volume move modify` com o `-cutover-action` parâmetro. O `volume move modify` comando é um comando avançado e o `-cutover-action` é um parâmetro avançado.

Consulte a página de manual de cada comando para obter mais informações.

Métodos para copiar um volume

O método usado para copiar um volume depende se você está copiando-o para o mesmo agregado ou para um agregado diferente e se deseja reter cópias Snapshot do volume original. Copiar um volume cria uma cópia autônoma de um volume que você pode usar para testes e outros fins.

A tabela a seguir lista as caraterísticas da cópia e os métodos usados para criar essa cópia.

Se quiser copiar um volume…	Então o método que você usa é…
Dentro do mesmo agregado e você não quer copiar cópias Snapshot do volume original.	Criar um volume FlexClone do volume original.
Para outro agregado e não quiser copiar cópias Snapshot do volume original.	Criando um volume FlexClone do volume original e movendo o volume para outro agregado usando o `volume move` comando.
Para outro agregado e preservar todas as cópias Snapshot do volume original.	Replicando o volume original usando o SnapMirror e quebrando a relação do SnapMirror para fazer uma cópia de volume de leitura e gravação.

Use o FlexClone volumes para criar cópias eficientes do seu FlexVol volumes

Visão geral do uso do volume do FlexClone

Os volumes FlexClone são cópias graváveis e pontuais de um FlexVol volume pai. Os volumes FlexClone usam espaço para uso eficiente, pois compartilham os mesmos blocos de dados com os volumes FlexVol pai para dados comuns. A cópia Snapshot usada para criar um volume FlexClone também é compartilhada com o volume pai.

Você pode clonar um volume FlexClone existente para criar outro volume FlexClone. Você também pode criar um clone de um FlexVol volume que contenha LUNs e clones de LUN.

Você também pode dividir um volume FlexClone de seu volume pai. A partir do ONTAP 9.4, para volumes não

garantidos em sistemas AFF, a operação dividida para volumes FlexClone compartilha os blocos físicos e não copia os dados. Portanto, a divisão de volumes FlexClone em sistemas AFF é mais rápida do que a operação de divisão FlexClone em outros sistemas FAS no ONTAP 9.4 e versões posteriores.

Você pode criar dois tipos de volumes FlexClone: Volumes FlexClone de leitura-gravação e volumes FlexClone de proteção de dados. Embora você possa criar um volume FlexClone de leitura e gravação de um FlexVol volume normal, use apenas um volume secundário do SnapVault para criar um volume FlexClone de proteção de dados.

Crie um volume FlexClone

Você pode criar um volume de FlexClone de proteção de dados a partir de um volume de destino do SnapMirror ou de um FlexVol volume pai que seja um volume secundário do SnapVault. A partir do ONTAP 9.7, é possível criar um volume FlexClone a partir de um volume FlexGroup. Depois de criar um volume FlexClone, não é possível excluir o volume pai enquanto o volume FlexClone existir.

Antes de começar

- A licença FlexClone deve ser instalada no cluster. Esta licença está incluída no "ONTAP One".
- O volume que você deseja clonar deve estar online.

> Clonar um volume como um volume FlexClone em um SVM diferente não é compatível com configurações do MetroCluster.

Crie um volume FlexClone de um FlexVol ou FlexGroup

Passo

1. Criar um volume FlexClone:

```
volume clone create
```

> Ao criar um volume FlexClone de leitura e gravação a partir do volume pai de leitura e gravação, não é necessário especificar a cópia Snapshot base. O ONTAP cria uma cópia Snapshot se você não nomear qualquer cópia Snapshot específica que deve ser usada como a cópia Snapshot de base para o clone. Você deve especificar a cópia Snapshot de base para criar um volume FlexClone quando o volume pai for um volume de proteção de dados.

Exemplo

- O comando a seguir cria um FlexClone volume vol1_clone de leitura-gravação a partir do volume pai vol1:

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume
vol1
```

- O comando a seguir cria uma proteção de dados FlexClone volume vol_dp_clone do volume pai dp_vol usando a cópia Snapshot base snap1:

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent
-volume dp_vol -parent-snapshot snap1
```

Crie um FlexClone de qualquer tipo de SnapLock

A partir do ONTAP 9.13,1, é possível especificar um dos três tipos de SnapLock, `compliance` `enterprise` `non-snaplock` , , , ao criar um FlexClone de um volume RW. Por padrão, um volume FlexClone é criado com o mesmo tipo de SnapLock que o volume pai. No entanto, você pode substituir o padrão usando a `snaplock-type` opção durante a criação de volume do FlexClone.

Usando o `non-snaplock` parâmetro com a `snaplock-type` opção, você pode criar um volume FlexClone de tipo não SnapLock a partir de um volume pai do SnapLock para fornecer um método mais rápido de colocar os dados novamente on-line quando necessário.

Saiba mais "SnapLock"sobre o .

Antes de começar

Você deve estar ciente das seguintes limitações de volume do FlexClone quando eles tiverem um tipo de SnapLock diferente do volume pai.

- Apenas clones do tipo RW são suportados. Clones do tipo DP com um tipo SnapLock diferente do volume pai não são suportados.
- Os volumes com LUNs não podem ser clonados usando a opção do tipo SnapLock definida para um valor diferente de "não-SnapLock" porque os volumes SnapLock não suportam LUNs.
- Um volume em um agregado espelhado MetroCluster não pode ser clonado com um tipo de SnapLock de conformidade porque os volumes SnapLock Compliance não são compatíveis com agregados espelhados do MetroCluster.
- Os volumes SnapLock Compliance com retenção legal não podem ser clonados com um tipo de SnapLock diferente. A retenção legal só é suportada em volumes SnapLock Compliance.
- O SVM DR não é compatível com SnapLock volumes. A tentativa de criar um clone de SnapLock a partir de um volume em um SVM que faça parte de uma relação SVM DR falhará.
- As práticas recomendadas da FabricPool recomendam que os clones mantenham a mesma política de disposição em camadas que os pais. No entanto, um clone do SnapLock Compliance de um volume habilitado para FabricPool não pode ter a mesma política de disposição em camadas que o pai. A política de disposição em categorias deve ser definida como `none`. A tentativa de criar um clone do SnapLock Compliance de um pai com uma política de disposição em camadas diferente `none` de falhará.

Passos

1. Criar um volume FlexClone com um tipo SnapLock: `volume clone create -vserver` *`svm_name`* `-flexclone` *`flexclone_name`* `-type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]`

   Exemplo:

   ```
   > volume clone create -vserver vs0 -flexclone vol1_clone -type RW
   -snaplock-type enterprise -parent-volume vol1
   ```

Divida um volume FlexClone do volume pai

Você pode dividir um volume FlexClone de seu pai para fazer o clone um FlexVol volume normal.

A operação de divisão de clones ocorre em segundo plano. Os dados podem ser acessados no clone e no pai durante a divisão. Começando com ONTAP 9.4, a eficiência de espaço é preservada. O processo de divisão atualiza apenas os metadados e requer o mínimo de e/S. Nenhum bloco de dados é copiado.

Sobre esta tarefa

- Não é possível criar novas cópias Snapshot do volume FlexClone durante a operação de divisão.
- Um volume FlexClone não pode ser dividido do volume pai se pertencer a uma relação de proteção de dados ou fizer parte de um espelhamento de compartilhamento de carga.
- Se você colocar o volume FlexClone offline enquanto a divisão estiver em andamento, a operação de divisão será suspensa; quando você colocar o volume FlexClone novamente on-line, a operação de divisão será retomada.
- Após a divisão, tanto o FlexVol volume pai quanto o clone exigem a alocação de espaço total determinada por suas garantias de volume.
- Depois que um volume FlexClone é dividido de seu pai, os dois não podem ser rejuntados.
- A partir do ONTAP 9.4, para volumes não garantidos em sistemas AFF, a operação dividida para volumes FlexClone compartilha os blocos físicos e não copia os dados. Portanto, a divisão de volumes FlexClone em sistemas AFF é mais rápida do que a operação de divisão FlexClone em outros sistemas FAS no ONTAP 9.4 e posterior. A operação de divisão de FlexClone aprimorada em sistemas AFF tem os seguintes benefícios:
  - A eficiência de storage é preservada após a divisão do clone do pai.
  - As cópias Snapshot existentes não são excluídas.
  - A operação é mais rápida.
  - O volume FlexClone pode ser dividido de qualquer ponto na hierarquia de clones.

Antes de começar

- Você deve ser um administrador de cluster.
- O volume FlexClone deve estar online quando a operação de divisão começar.
- O volume principal deve estar online para que a divisão tenha sucesso.

Passos

1. Determine a quantidade de espaço livre necessária para concluir a operação de divisão:

   `volume clone show -estimate -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`* `-parent-volume` *`parent_vol_name`*

   O exemplo a seguir fornece informações sobre o espaço livre necessário para dividir o volume FlexClone "'clone1" do volume pai "'vol1":

   ```
   cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1
   -parent-volume volume1
                               Split
   Vserver   FlexClone       Estimate
   --------- ------------- ----------
   vs1       clone1           40.73MB
   ```

2. Verifique se o agregado que contém o volume FlexClone e seu pai tem espaço suficiente:

a. Determine a quantidade de espaço livre no agregado que contém o volume FlexClone e seu pai:

   `storage aggregate show`

b. Se o agregado que contém não tiver espaço livre suficiente disponível, adicione armazenamento ao agregado:

   `storage aggregate add-disks`

3. Inicie a operação dividida:

   `volume clone split start -vserver vserver_name -flexclone clone_volume_name`

   O exemplo a seguir mostra como você pode iniciar o processo para dividir o volume FlexClone "'clone1" do volume pai "'vol1":

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

4. Monitorize o estado da operação dividida do FlexClone:

   `volume clone split show -vserver vserver_name -flexclone clone_volume_name`

   O exemplo a seguir mostra o status da operação dividida do FlexClone em um sistema AFF:

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
                                              Inodes
Blocks
                                    ----------------------
----------------------
Vserver   FlexClone    Processed Total    Scanned  Updated      % Inode
% Block

Complete  Complete
vs1       clone1        0         0       411247   153600         0
37
```

5. Verifique se o volume de divisão não é mais um volume FlexClone:

   `volume show -volume volume_name -fields clone-volume`

   O valor `clone-volume` da opção é "false" para um volume que não é um volume FlexClone.

   O exemplo a seguir mostra como você pode verificar se o volume "'clone1" que está dividido de seu pai

não é um volume FlexClone.

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
------- ------ **-------------**
vs1     clone1 **false**
```

Determine o espaço usado por um volume FlexClone

É possível determinar o espaço usado por um volume FlexClone com base no tamanho nominal e na quantidade de espaço que ele compartilha com o FlexVol volume pai. Quando um volume FlexClone é criado, ele compartilha todos os dados com o volume pai. Embora o tamanho nominal do FlexVol volume seja o mesmo que o tamanho de seu pai, ele usa muito pouco espaço livre do agregado.

Sobre esta tarefa

O espaço livre usado por um volume FlexClone recém-criado é de aproximadamente 0,5% de seu tamanho nominal. Esse espaço é usado para armazenar os metadados do volume FlexClone.

Os novos dados gravados no volume pai ou no FlexClone não são compartilhados entre os volumes. O aumento na quantidade de novos dados gravados no volume FlexClone leva a um aumento no espaço que o volume FlexClone requer do agregado que contém.

Passo

1. Determine o espaço físico real usado pelo volume FlexClone usando o `volume show` comando.

   O exemplo a seguir mostra o espaço físico total usado pelo volume FlexClone:

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver    volume     size  available  used   percent-used   physical-
used     physical-used-percent
-------   ----------  ----  ---------  -----  ------------
-------------   ---------------------
vs01     clone_vol1   20MB   18.45MB   564KB       7%             196KB
1%
```

Considerações para criar um volume FlexClone a partir de uma fonte ou volume de destino SnapMirror

Você pode criar um volume FlexClone a partir do volume de origem ou destino em uma relação de volume SnapMirror existente. No entanto, isso pode impedir que futuras operações de replicação do SnapMirror sejam concluídas com êxito.

A replicação pode não funcionar porque ao criar o volume FlexClone, você pode bloquear uma cópia Snapshot usada pelo SnapMirror. Se isso acontecer, o SnapMirror pára de replicar para o volume de destino

até que o volume FlexClone seja destruído ou seja dividido de seu pai. Você tem duas opções para resolver este problema:

- Se você precisar do volume FlexClone temporariamente e puder acomodar uma parada temporária da replicação do SnapMirror, poderá criar o volume FlexClone e excluí-lo ou dividi-lo de seu pai quando possível.

  A replicação SnapMirror continua normalmente quando o volume FlexClone é excluído ou é dividido de seu pai.

- Se uma interrupção temporária da replicação do SnapMirror não for aceitável, você poderá criar uma cópia Snapshot no volume de origem do SnapMirror e usá-la para criar o volume FlexClone. (Se você estiver criando o volume FlexClone a partir do volume de destino, aguarde até que a cópia Snapshot seja replicada para o volume de destino do SnapMirror.)

  Esse método de criação de uma cópia Snapshot no volume de origem do SnapMirror permite criar o clone sem bloquear uma cópia Snapshot que esteja em uso pelo SnapMirror.

Use arquivos FlexClone e LUNs FlexClone para criar cópias eficientes de arquivos e LUNs

Visão geral do uso do arquivo FlexClone e do FlexClone LUN

Os arquivos FlexClone e os LUNs FlexClone são clones graváveis, com uso eficiente de espaço, de arquivos pai e LUNs pai, além de ajudar na utilização eficiente do espaço agregado físico. O FlexClone Files e os FlexClone LUNs são compatíveis apenas com volumes FlexVol.

Os arquivos FlexClone e os LUNs FlexClone utilizam 0,4% do tamanho deles para armazenar os metadados. Os clones compartilham os blocos de dados de seus arquivos pai e LUNs pai e ocupam espaço de storage insignificante até que os clientes gravem novos dados no arquivo pai ou LUN ou no clone.

Os clientes podem executar todas as operações de arquivo e LUN nas entidades pai e clone.

Você pode usar vários métodos para excluir arquivos FlexClone e LUNs FlexClone.

Crie um arquivo FlexClone ou FlexClone LUN

Use o comando para criar clones com uso eficiente de espaço e tempo de arquivos e LUNs presentes no FlexVol volumes ou no FlexClone volumes `volume file clone create`.

O que você vai precisar

- A licença FlexClone deve ser instalada no cluster. Esta licença está incluída no "ONTAP One".
- Se vários intervalos de blocos forem usados para clonagem de sub-LUN ou clonagem de sub-arquivo, os números de bloco não devem se sobrepor.
- Se você estiver criando um sub-LUN ou sub-arquivo em volumes com compactação adaptável ativada, os intervalos de bloco não devem ser desalinhados.

  Isso significa que o número do bloco de início da origem e o número do bloco de início de destino devem estar alinhados ou alinhados de forma ímpar.

Sobre esta tarefa

Dependendo do Privileges atribuído pelo administrador do cluster, um administrador da SVM pode criar arquivos FlexClone e LUNs FlexClone.

É possível especificar a configuração de FlexClone Files e FlexClone LUNs quando você cria e modifica clones. Por predefinição, a definição de velocidade de cruzeiro é desativada.

Você pode sobrescrever um arquivo FlexClone existente ou LUN FlexClone ao criar um clone usando o `volume file clone create` comando com o `-overwrite-destination` parâmetro.

Quando o nó atinge sua carga dividida máxima, o nó pára temporariamente de aceitar solicitações para criar arquivos FlexClone e LUNs FlexClone e emite uma `EBUSY` mensagem de erro. Quando a carga dividida para o nó cai abaixo do máximo, o nó aceita solicitações para criar arquivos FlexClone e LUNs FlexClone novamente. Você deve esperar até que o nó tenha capacidade para criar os clones antes de tentar a solicitação de criação novamente.

Passos

1. Crie um arquivo FlexClone ou FlexClone LUN usando o `volume file clone create` comando.

   O exemplo a seguir mostra como você pode criar um arquivo FlexClone file1_clone do arquivo pai file1_source no volume vol1:

   ```
   cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
   -path /file1_source -destination-path /file1_clone
   ```

   Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Informações relacionadas

"Referência do comando ONTAP"

Visualize a capacidade do nó antes de criar e excluir arquivos FlexClone e LUNs FlexClone

Você deve determinar se um nó tem capacidade para receber solicitações para criar e excluir arquivos FlexClone e LUNs FlexClone. Isso pode ser feito visualizando a carga dividida para o nó. Se a carga máxima de divisão for atingida, não serão aceites novos pedidos até que a carga dividida fique abaixo do máximo.

Sobre esta tarefa

Quando o nó atinge sua carga máxima de divisão, uma `EBUSY` mensagem de erro é emitida em resposta à criação e exclusão de solicitações. Quando a carga dividida para o nó cai abaixo do máximo, o nó aceita solicitações para criar e excluir arquivos FlexClone e LUNs FlexClone novamente.

Um nó pode aceitar novas solicitações quando o `Allowable Split Load` campo exibe capacidade e a solicitação de criação se encaixa na capacidade disponível.

Passos

1. Veja a quantidade de capacidade que um nó tem para criar e excluir arquivos FlexClone e LUNs FlexClone usando o `volume file clone split load show` comando.

   No exemplo a seguir, a carga dividida é exibida para todos os nós em cluster1. Todos os nós no cluster

têm capacidade para criar e excluir arquivos FlexClone e LUNs FlexClone, conforme indicado pelo campo carga dividida permitida:

```
cluster1::> volume file clone split load show
Node       Max         Current    Token          Allowable
           Split Load  Split Load Reserved Load  Split Load
---------- ----------  ---------- -------------  ----------
node1         15.97TB          0B          100MB    15.97TB
node2         15.97TB          0B          100MB    15.97TB
2 entries were displayed.
```

Visualize economia de espaço com arquivos FlexClone e LUNs FlexClone

É possível exibir a porcentagem de espaço em disco salvo pelo compartilhamento de blocos em um volume que contém arquivos FlexClone e LUNs FlexClone. Você pode fazer isso como parte do Planejamento de capacidade.

Passos

1. Para visualizar a economia de espaço alcançada devido a arquivos FlexClone e LUNs FlexClone, digite o seguinte comando:

   `df -s volname`

   `volname` É o nome do FlexVol volume.

   Se você executar o `df -s` comando em um FlexVol volume habilitado para deduplicação, poderá visualizar o espaço economizado tanto por arquivos de deduplicação quanto por FlexClone e LUNs.

Exemplo

O exemplo a seguir mostra a economia de espaço em um volume FlexClone test1:

```
systemA> df -s test1

Filesystem         used   saved   %saved Vserver
/vol/test1/        4828    5744     54%  vs1
```

Métodos para excluir arquivos FlexClone e LUNs FlexClone

Você pode usar vários métodos para excluir arquivos FlexClone e LUNs FlexClone. Entender quais métodos estão disponíveis ajuda você a Planejar como gerenciar clones.

Você pode usar os seguintes métodos para excluir arquivos FlexClone e LUNs FlexClone:

- Você pode configurar um FlexVol volume para excluir automaticamente clones com o recurso de transferência de dados ativado quando o espaço livre em um FlexVol volume diminuir abaixo de um

determinado limite.

- Você pode configurar clientes para excluir clones usando o SDK de gerenciabilidade do NetApp.
- Você pode usar clientes para excluir clones usando os protocolos nas e SAN.

  O método de exclusão mais lento é habilitado por padrão porque esse método não usa o SDK de gerenciamento do NetApp. No entanto, você pode configurar o sistema para usar o método de exclusão mais rápido quando você excluir arquivos FlexClone usando os `volume file clone deletion` comandos.

Como um FlexVol volume pode recuperar espaço livre com a configuração de transferência de dados

Volumes do FlexVol e recuperação de espaço livre com visão geral do projeto

Pode ativar a definição de FlexVol volume para eliminar automaticamente ficheiros FlexClone e LUNs FlexClone. Ao ativar o serviço de correio eletrónico, pode recuperar uma quantidade alvo de espaço livre no volume quando um volume estiver quase cheio.

Você pode configurar um volume para começar a excluir automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminuir abaixo de um determinado valor limite e parar automaticamente de excluir clones quando uma quantidade de espaço livre no volume for recuperada. Embora não seja possível especificar o valor de limite que inicia a exclusão automática de clones, você pode especificar se um clone é elegível para exclusão e especificar a quantidade de espaço livre de destino para um volume.

Um volume exclui automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminui abaixo de um determinado limite e quando *ambos* dos seguintes requisitos são atendidos:

- A funcionalidade de autodelete está ativada para o volume que contém os arquivos FlexClone e LUNs FlexClone.

  Você pode ativar a capacidade de transferência de um FlexVol volume usando o `volume snapshot autodelete modify` comando. Você deve definir o `-trigger` parâmetro para `volume` ou `snap_reserve` para que um volume exclua automaticamente arquivos FlexClone e LUNs FlexClone.

- A funcionalidade de configuração do sistema de áudio e vídeo é habilitada para os LUNs FlexClone e FlexClone.

  Você pode ativar o arquivo FlexClone ou FlexClone LUN usando o `file clone create` comando com o `-autodelete` parâmetro. Como resultado, você pode preservar certos arquivos FlexClone e LUNs FlexClone, desativando o serviço de seleção de clones e garantindo que outras configurações de volume não substituam a configuração de clone.

Configure um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone

Você pode habilitar um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminuir abaixo de um determinado limite.

O que você vai precisar

- O FlexVol volume deve conter arquivos FlexClone e LUNs FlexClone, além de estar online.
- O FlexVol volume não deve ser um volume somente leitura.

Passos

1. Ative a exclusão automática de arquivos FlexClone e LUNs FlexClone no FlexVol volume usando o `volume snapshot autodelete modify` comando.
   - Para o `-trigger` parâmetro, pode especificar `volume` ou `snap_reserve`.
   - Para o `-destroy-list` parâmetro, você deve sempre especificar `lun_clone,file_clone`, independentemente de você querer excluir apenas um tipo de clone. O exemplo a seguir mostra como você pode ativar o volume vol1 para acionar a exclusão automática de arquivos FlexClone e LUNs FlexClone para recuperação de espaço até que 25% do volume consista em espaço livre:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

   > Ao ativar volumes FlexVol para exclusão automática, se você definir o valor `-commitment` do parâmetro como `destroy`, todos os arquivos FlexClone e LUNs FlexClone com o `-autodelete` parâmetro definido como `true` poderão ser excluídos quando o espaço livre no volume diminuir abaixo do valor de limite especificado. No entanto, os arquivos FlexClone e LUNs FlexClone com o `-autodelete` parâmetro definido como `false` não serão excluídos.

2. Verifique se a exclusão automática de arquivos FlexClone e LUNs FlexClone está ativada no FlexVol volume usando o `volume snapshot autodelete show` comando.

   O exemplo a seguir mostra que o volume vol1 está habilitado para exclusão automática de arquivos FlexClone e LUNs FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
           Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)
    Target Free Space: 25%
              Trigger: volume
     *Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. Certifique-se de que o serviço de correio eletrónico está ativado para os ficheiros FlexClone e LUNs FlexClone no volume que pretende eliminar, executando as seguintes etapas:
   a. Ative a exclusão automática de um arquivo FlexClone específico ou LUN FlexClone usando o `volume`

`file clone autodelete` comando.

Você pode forçar um arquivo FlexClone específico ou LUN FlexClone a ser automaticamente excluído usando o `volume file clone autodelete` comando com o `-force` parâmetro.

O exemplo a seguir mostra que a exclusão automática do FlexClone LUN lun1_clone contido no volume vol1 está ativada:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

Você pode ativar o arquivo FlexClone e LUNs do FlexClone.

b. Verifique se o arquivo FlexClone ou FlexClone LUN está habilitado para exclusão automática usando o `volume file clone show-autodelete` comando.

O exemplo a seguir mostra que o FlexClone LUN lun1_clone está habilitado para exclusão automática:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
**Autodelete Enabled: true**
```

Para obter mais informações sobre como usar os comandos, consulte as respetivas páginas de manual.

Impedir a eliminação automática de um ficheiro FlexClone ou LUN FlexClone

Se você configurar um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone, qualquer clone que atenda aos critérios especificados poderá ser excluído. Se você tiver arquivos FlexClone ou LUNs FlexClone específicos que deseja preservar, poderá excluí-los do processo de exclusão automática do FlexClone.

Antes de começar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

Quando você cria um arquivo FlexClone ou LUN FlexClone, por padrão, a configuração de ciclo de vida para o clone é desativada. Os arquivos do FlexClone e os LUNs do FlexClone com o recurso de configuração de ciclo de vida desativado são preservados quando você configura um FlexVol volume para excluir automaticamente clones para recuperar espaço no volume.

> Se você definir o `commitment` nível no volume como `try` ou `disrupt`, poderá preservar individualmente arquivos FlexClone ou LUNs FlexClone específicos desativando o modo de exibição de dados para esses clones. No entanto, se você definir o `commitment` nível no volume como `destroy` e as listas destruir incluir `lun_clone,file_clone`, a configuração de volume substituirá a configuração clone e todos os arquivos FlexClone e FlexClone LUNs poderão ser excluídos independentemente da configuração de ciclo de vida dos clones.

Passos

1. Evite que um arquivo FlexClone específico ou LUN FlexClone seja excluído automaticamente usando o `volume file clone autodelete` comando.

   O exemplo a seguir mostra como você pode desativar o FlexClone LUN lun1_clone contido no vol1:

   ```
   cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
   -clone-path lun1_clone -enable false
   ```

   Um arquivo ou LUN FlexClone com o sistema de diagnóstico guiado por sintomas (FlexClone) desativado não pode ser excluído automaticamente para recuperar espaço no volume.

2. Verifique se o arquivo FlexClone ou FlexClone LUN está desabilitado usando o `volume file clone show-autodelete` comando.

   O exemplo a seguir mostra que o FlexClone lun lun1_clone é falso:

   ```
   cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
   vol/vol1/lun1_clone
                                                                  Vserver
   Name: vs1
                                                                  Clone Path:
   vol/vol1/lun1_clone
                                                                  Autodelete
   Enabled: false
   ```

Comandos para configurar a exclusão de arquivos FlexClone

Quando os clientes excluem arquivos FlexClone sem usar o SDK de gerenciamento do NetApp, você pode usar os `volume file clone deletion` comandos para permitir a exclusão mais rápida de arquivos FlexClone de um FlexVol volume. Extensões e tamanho mínimo de arquivos FlexClone são usados para permitir a exclusão mais rápida.

Você pode usar os `volume file clone deletion` comandos para especificar uma lista de extensões suportadas e um requisito de tamanho mínimo para arquivos FlexClone em um volume. O método de exclusão mais rápido é usado apenas para arquivos FlexClone que atendam aos requisitos. Para arquivos FlexClone que não atendem aos requisitos, o método de exclusão mais lento é usado.

Quando os clientes excluem arquivos FlexClone e LUNs FlexClone de um volume usando o SDK de gerenciamento do NetApp, os requisitos de extensão e tamanho não se aplicam porque o método de exclusão mais rápido é sempre usado.

Para…	Use este comando…
Adicione uma extensão à lista de extensões suportadas para o volume	`volume file clone deletion add-extension`
Altere o tamanho mínimo dos arquivos FlexClone que podem ser excluídos do volume usando o método de exclusão mais rápido	`volume file clone deletion modify`
Remova uma extensão da lista de extensões suportadas para o volume	`volume file clone deletion remove-extension`
Visualize a lista de extensões suportadas e o tamanho mínimo de ficheiros FlexClone que os clientes podem eliminar do volume utilizando o método de eliminação mais rápida	`volume file clone deletion show`

Para obter informações detalhadas sobre esses comandos, consulte a página man apropriada.

Use qtrees para particionar seus volumes FlexVol

Qtrees e particionamento de ONTAP FlexVol volume

Qtrees permitem que você particione volumes FlexVol em segmentos menores que podem ser gerenciados individualmente. O particionamento de volume habilitado pelo qtrees fornece um nível mais fino de controle ao administrar o storage por projeto, usuário ou grupo. Você pode usar qtrees para gerenciar melhor cotas, estilo de segurança e plocks CIFS.

O ONTAP cria uma qtree padrão para cada volume chamado **qtree0**. Se você não colocar dados em uma qtree específico, ele será colocado em qtree0.

Limitações gerais

Você deve estar ciente das limitações de qtrees antes de usá-los em um ambiente de produção. Revise também o Funcionamento e limitações quando usar o recurso de monitoramento de desempenho de qtree estendido.

- Os nomes Qtree não podem ter mais de 64 carateres.
- Certos carateres especiais usados nos nomes de qtree, como vírgulas e espaços, podem causar problemas com outros recursos do ONTAP e devem ser evitados.
- Você não pode mover diretórios entre diferentes qtrees. Somente arquivos podem ser movidos entre qtrees.
- Se você criar compartilhamentos em nível de qtree e em nível de volume no mesmo pool FlexVol ou SCVMM, o qtrees aparecerá como diretórios no compartilhamento FlexVol. Você deve ter cuidado para não excluí-los acidentalmente.

Comandos para gerenciar e configurar qtrees

Você pode gerenciar e configurar qtrees usando a CLI do ONTAP. Dependendo do que você quer fazer, você deve usar os seguintes comandos para administrar qtrees.

> O comando `volume rehost` pode fazer com que outras operações administrativas simultâneas direcionadas ao mesmo volume falhem.

Se você quiser…	Use este comando…
Crie uma qtree	`volume qtree create`
Exibir uma lista filtrada de qtrees	`volume qtree show`
Eliminar uma qtree	`volume qtree delete` > Este comando falhará a menos que a qtree esteja vazia ou que a `-force true` bandeira seja usada.
Modifique as permissões UNIX de uma qtree	`volume qtree modify -unix-permissions`
Modifique a configuração dos oplocks CIFS de uma qtree	`volume qtree oplocks`
Modifique a configuração de segurança de uma qtree	`volume qtree security`
Renomeie uma qtree	`volume qtree rename`
Apresentar as estatísticas de uma qtree	`volume qtree statistics`
Redefinir as estatísticas de uma qtree	`volume qtree statistics -reset`

Monitoramento de desempenho de qtree estendido

A partir do ONTAP 9.16,1, você pode usar a API REST do ONTAP para acessar os recursos estendidos de monitoramento de qtree, que incluem métricas de latência e estatísticas históricas.

A API REST do ONTAP inclui vários endpoints relacionados ao qtrees. Antes do ONTAP 9.16,1, os clientes podiam acessar estatísticas em tempo real para qtrees, incluindo operações de e/S por segundo (IOPs), bem como taxa de transferência para operações de leitura, gravação e outras.

O monitoramento de desempenho estendido de qtree disponível a partir do ONTAP 9.16,1 permite monitorar estatísticas de latência em tempo real, além de IOPs e taxa de transferência para NFSv3, NFSv4,0, NFSv4,1, NFSv4,2, pNFS (tecnicamente parte do NFSv4,1 e NFSv4,2) e CIFS. Ele também coleta e arquiva estatísticas para permitir a visualização de dados históricos de desempenho.

Esse monitoramento estendido fornece aos administradores de storage maiores insights sobre a performance

do sistema. Você pode usar esses dados para identificar qtrees de alto uso, gargalos potenciais e outras áreas ao trabalhar para melhorar a qualidade do serviço. Ser capaz de analisar essas métricas, incluindo tendências por um período mais longo, permite que você tome decisões mais informadas baseadas em dados.

Funcionamento e limitações

Há várias caraterísticas operacionais, incluindo limitações, que você deve considerar antes de usar o recurso de monitoramento de desempenho de qtree estendido em um ambiente de produção.

Remontagem necessária

Depois de ativar o monitoramento estendido de qtree, você precisa remontar o volume afetado para ativar o recurso.

Disponibilidade de estatísticas

Depois de permitir uma monitorização alargada do desempenho, os dados estatísticos não estão imediatamente disponíveis. Isso inclui estatísticas de IOPS, taxa de transferência e latência. Pode levar até cinco minutos antes que esses dados sejam exibidos para uma qtree.

Qtrees por cluster

Você pode ativar o monitoramento de desempenho estendido para um máximo de 50.000 qtrees em um cluster ONTAP.

Acesse métricas estendidas usando a API REST do ONTAP

A partir do ONTAP 9.16,1, você pode acessar o recurso de monitoramento de desempenho de qtree estendido por meio da API REST do ONTAP. Os recursos básicos se enquadram em várias categorias, conforme descrito abaixo.

Ative e desative o monitoramento de desempenho estendido

Você pode acessar a propriedade `ext_performance_monitoring.enabled` no endpoint `/api/storage/qtrees` para ativar ou desativar o recurso de monitoramento estendido. Os métodos POST e PATCH estão disponíveis dependendo se você está criando uma nova qtree ou configurando uma qtree existente.

Recupere métricas e configurações de monitoramento globais

Várias novas propriedades globais foram adicionadas ao `/api/storage/qtrees` endpoint. Você pode recuperar esses campos usando o método GET.

Recuperar métricas para uma qtree específico

Você pode usar o método GET no endpoint `/api/storage/qtrees/{volume.uuid}/{id}/metrics` para recuperar as novas propriedades de estatísticas e métricas para uma qtree específico, conforme definido em um volume específico.

Atualizando e revertendo

Se ativar a funcionalidade no ONTAP 9.16,1, pode atualizar para uma versão subsequente do ONTAP sem restrições. No entanto, existem dois cenários a considerar.

Atualize para 9.16.1 e manipule clusters de versão mista

O recurso de monitoramento de desempenho estendido não pode ser usado (ou seja, `ext_performance_monitoring.enabled` não pode ser definido como `true`) até que a versão de cluster efetiva (ECV) do cluster esteja em 9.16.1.

Reverter de 9.16.1

Se qualquer qtrees tiver a propriedade `ext_performance_monitoring.enabled` definida como `true`, reverter para 9.15.1 de 9.16.1 não é permitido. A operação de reversão está bloqueada. A melhor prática é `ext_performance_monitoring.enabled` definir como `false` para todos os qtrees antes de reverter para uma versão anterior do ONTAP.

Saiba mais

Saiba mais sobre a API REST do ONTAP, incluindo "Novidades com a API REST do ONTAP", na documentação de automação do ONTAP. Você também deve consultar a documentação de automação do ONTAP para obter detalhes sobre a API REST do ONTAP "endpoints de qtree" .

Obtenha um caminho de junção de qtree

Você pode montar uma qtree individual obtendo o caminho de junção ou caminho de namespace da qtree. O caminho de qtree exibido pelo comando CLI `qtree show -instance` é do formato `/vol/<volume_name>/<qtree_name>`. No entanto, esse caminho não se refere ao caminho de junção ou caminho de namespace da qtree.

Sobre esta tarefa

Você precisa saber o caminho de junção do volume para obter o caminho de junção ou caminho de namespace da qtree.

Passos

1. Use o `vserver volume junction-path` comando para obter o caminho de junção de um volume.

   O exemplo a seguir exibe o caminho de junção do volume chamado vol1 localizado na máquina virtual de armazenamento (SVM) chamada vs0:

   ```
   cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

   ------- ------ -------------

   vs0 vol1 /vol1
   ```

   A partir da saída acima, o caminho de junção do volume é `/vol1`. Como qtrees são sempre enraizados no volume, o caminho de junção ou o caminho do namespace da qtree será `/vol1/qtree1`.

Conversões de diretório para qtree

Converta um diretório em uma qtree

Se você tiver um diretório na raiz de um FlexVol volume que deseja converter em uma qtree, precisará migrar os dados contidos no diretório para uma nova qtree com o mesmo nome, usando seu aplicativo cliente.

Sobre esta tarefa

As etapas que você seguir para converter um diretório em uma qtree dependem do cliente que você usa. O

processo a seguir descreve as tarefas gerais que você precisa concluir.

Antes de começar

Não é possível excluir um diretório se ele estiver associado a um compartilhamento CIFS existente.

Passos

1. Renomeie o diretório a ser transformado em uma qtree.
2. Crie uma nova qtree com o nome do diretório original.
3. Use o aplicativo cliente para mover o conteúdo do diretório para a nova qtree.
4. Exclua o diretório agora vazio.

Converta um diretório em uma qtree usando um cliente Windows

Para converter um diretório em uma qtree usando um cliente Windows, renomeie o diretório, crie uma qtree no sistema de armazenamento e mova o conteúdo do diretório para a qtree.

Sobre esta tarefa

Você deve usar o Windows Explorer para este procedimento. Você não pode usar a interface de linha de comando do Windows ou o ambiente de prompt do dos.

Passos

1. Abra o Explorador do Windows.
2. Clique na representação da pasta do diretório que deseja alterar.

   O diretório deve residir na raiz de seu volume contendo.

3. No menu **File**, selecione **Renomear** para atribuir um nome diferente a este diretório.
4. No sistema de armazenamento, use o `volume qtree create` comando para criar uma nova qtree com o nome original do diretório.
5. No Windows Explorer, abra a pasta de diretório renomeada e selecione os arquivos dentro dela.
6. Arraste esses arquivos para a representação da pasta da nova qtree.

   Quanto mais subpastas contidas na pasta que você está movendo, mais longa a operação de movimentação demora.

7. No menu **Arquivo**, selecione **Excluir** para excluir a pasta de diretório renomeada, agora vazia.

Converta um diretório em uma qtree usando um cliente UNIX

Para converter um diretório para uma qtree no UNIX, renomeie o diretório, crie uma qtree no sistema de armazenamento e mova o conteúdo do diretório para a qtree.

Passos

1. Abra uma janela do cliente UNIX.
2. Use o `mv` comando para renomear o diretório.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. No sistema de armazenamento, use o `volume qtree create` comando para criar uma qtree com o nome original.

```
system1: volume qtree create /n/user1/vol1/dir1
```

4. A partir do cliente, use o `mv` comando para mover o conteúdo do diretório antigo para a qtree.

> Quanto mais subdiretórios contidos em um diretório que você está movendo, mais longa a operação mover levará.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. Use o `rmdir` comando para excluir o diretório antigo, agora vazio.

```
client: rmdir /n/user1/vol1/olddir
```

Depois de terminar

Dependendo de como seu cliente UNIX implementa o `mv` comando, a propriedade do arquivo e as permissões podem não ser preservadas. Se isso ocorrer, atualize os proprietários de arquivos e as permissões para seus valores anteriores.

Relatórios de espaço lógico e imposição para volumes

Relatórios de espaço lógico e imposição para visão geral de volumes

A partir do ONTAP 9.4, é possível permitir que o espaço lógico usado em um volume e a quantidade de espaço de armazenamento restante sejam exibidos aos usuários. Começando com ONTAP 9.5, você pode limitar a quantidade de espaço lógico consumida pelos usuários.

O relatório e a imposição de espaços lógicos são desativados por padrão.

Os seguintes tipos de volume suportam relatórios e aplicação de espaço lógico.

Tipo de volume	Os relatórios de espaço são suportados?	A aplicação do espaço é suportada?
Volumes FlexVol	Sim, começando com ONTAP 9.4	Sim, começando com ONTAP 9.5
Volumes de destino do SnapMirror	Sim, começando com ONTAP 9.8	Sim, começando com ONTAP 9.13,1

Tipo de volume	Os relatórios de espaço são suportados?	A aplicação do espaço é suportada?
Volumes FlexGroup	Sim, começando com ONTAP 9.9,1	Sim, começando com ONTAP 9.9,1
Volumes FlexCache	A configuração de origem é usada no cache	Não aplicável

Imposição de espaço lógico

A aplicação de espaço lógico garante que os usuários sejam notificados quando um volume estiver cheio ou quase cheio. Quando você ativa a imposição de espaço lógico no ONTAP 9.5 e posterior, o ONTAP conta os blocos usados em um volume para determinar a quantidade de espaço que ainda está disponível nesse volume. Se não houver espaço disponível em um volume, o sistema retornará uma mensagem de erro ENOSPC (out-of-space).

A aplicação de espaço lógico retorna três tipos de alertas para informá-lo sobre o espaço disponível em um volume:

- `Monitor.vol.full.inc.sav`: Este alerta é acionado quando 98% do espaço lógico no volume tiver sido utilizado.
- `Monitor.vol.nearFull.inc.sav`: Este alerta é acionado quando 95% do espaço lógico no volume tiver sido utilizado.
- `Vol.log.overalloc.inc.sav`: Este alerta é acionado quando o espaço lógico utilizado no volume é superior ao tamanho total do volume.

  Esse alerta informa que adicionar ao tamanho do volume pode não criar espaço disponível, já que esse espaço já será consumido por blocos lógicos superalocados.

ⓘ O total (espaço lógico) deve ser igual ao espaço provisionado, excluindo a reserva Snapshot do volume com imposição de espaço lógico.

Para obter mais informações, "Configurar volumes para fornecer automaticamente mais espaço quando estiverem cheios"consulte .

Relatórios de espaço lógico

Quando você ativa o relatório de espaço lógico em um volume, seu sistema pode exibir a quantidade de espaço lógico usado e disponível, além do espaço total em um volume. Além disso, os usuários em sistemas cliente Linux e Windows podem ver espaço lógico usado e disponível em vez de espaço físico usado e físico disponível.

Definições:

- O espaço físico refere-se aos blocos físicos de armazenamento disponíveis ou usados no volume.
- O espaço lógico refere-se ao espaço utilizável em um volume.
- O espaço lógico usado é o espaço físico usado, além de economia com recursos de eficiência de storage

(como deduplicação e compactação) configurados.

A partir do ONTAP 9.5, você pode ativar a aplicação de espaço lógico juntamente com relatórios de espaço.

Quando ativado, o relatório de espaço lógico exibe os seguintes parâmetros com o `volume show` comando:

Parâmetro	Significado
`-logical-used`	Exibe informações somente sobre o volume ou volumes que têm o tamanho lógico usado especificado. Esse valor inclui todo o espaço economizado pelos recursos de eficiência de storage, juntamente com o espaço usado fisicamente. Isso não inclui a reserva Snapshot, mas considera o derramamento de Snapshot.
`-logical-used-by-afs`	Exibe informações apenas sobre o volume ou volumes que têm o tamanho lógico especificado usado pelo sistema de arquivos ativo. Esse valor difere do `-logical-used` valor pela quantidade de derramamento de Snapshot que excede a reserva de snapshot.
`-logical-available`	Quando apenas o relatório de espaço lógico está ativado, apenas o espaço físico disponível é exibido. Quando o relatório de espaço e a imposição estão ativados, ele exibe a quantidade de espaço livre atualmente disponível considerando o espaço economizado pelos recursos de eficiência de storage como sendo usado. Isso não inclui a reserva Snapshot.
`-logical-used -percent`	Exibe a porcentagem do valor atual `-logical-used` com o tamanho provisionado, excluindo a reserva Snapshot do volume. Esse valor pode ser superior a 100%, pois o `-logical-used-by-afs` valor inclui economia de eficiência no volume. `-logical-used-by-afs`O valor de um volume não inclui derramamento de Snapshot como espaço usado. `-physical-used`O valor de um volume inclui derramamento de Snapshot como espaço usado.
`-used`	Exibe a quantidade de espaço ocupado pelos dados do usuário e metadados do sistema de arquivos. Ele difere `physical-used` do espaço pela soma do espaço reservado para gravações futuras e do espaço economizado pela eficiência de storage agregado. Isso inclui derramamento de Snapshot (a quantidade de espaço em que as cópias Snapshot excedem a reserva Snapshot). Ele não inclui a reserva Snapshot.

A ativação de relatórios de espaço lógico na CLI também permite que os valores de espaço lógico usado (%) e espaço lógico sejam exibidos no System Manager

Os sistemas clientes veem o espaço lógico exibido como espaço "usado" nas seguintes telas do sistema:

- Saída **DF** em sistemas Linux
- Detalhes do espaço em Propriedades usando o Windows Explorer em sistemas Windows.

Se o relatório de espaço lógico estiver ativado sem imposição de espaço lógico, o total exibido nos sistemas cliente pode ser maior do que o espaço provisionado.

Ativar relatórios e imposição de espaço lógico

A partir do ONTAP 9.4, você pode ativar o relatório de espaço lógico. A partir do 9,5, você pode habilitar a aplicação de espaço lógico, ou tanto relatórios quanto imposição juntos.

Sobre esta tarefa

Além de ativar a aplicação e a geração de relatórios de espaço lógico no nível de volume individual, você pode habilitá-los no nível SVM para cada volume compatível com a funcionalidade. Se você habilitar recursos de espaço lógico para toda a SVM, também poderá desativá-los para volumes individuais.

A partir do ONTAP 9.8, se você ativar a geração de relatórios de espaço lógico em um volume de origem SnapMirror, ele será automaticamente ativado no volume de destino após a transferência.

A partir do ONTAP 9.13,1, se a opção de imposição estiver ativada em um volume de origem SnapMirror, o destino informará o consumo de espaço lógico e honrará sua aplicação, permitindo um melhor Planejamento de capacidade.

> Se você estiver executando uma versão do ONTAP anterior ao ONTAP 9.13,1, você deve entender que, embora a configuração de imposição seja transferida para o volume de destino do SnapMirror, o volume de destino não oferece suporte à imposição. Como resultado, o destino reportará o consumo de espaço lógico, mas não honrará sua aplicação.

Saiba mais "Suporte à versão ONTAP para relatórios de espaço lógico"sobre o .

Passos

Ative uma ou mais das seguintes opções:

- Ativar relatórios de espaço lógico para um volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true
```

- Ativar a imposição de espaço lógico para um volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-enforcement-logical true
```

- Ative relatórios de espaço lógico e imposição juntos para um volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true -is-space-enforcement-logical true
```

- Habilite a aplicação ou geração de relatórios de espaço lógico para um novo SVM:

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

- Habilite a aplicação ou a geração de relatórios de espaço lógico para uma SVM existente:

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

Gerenciar limites de capacidade do SVM

A partir do ONTAP 9.13,1, é possível definir a capacidade máxima para uma VM de storage (SVM). Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite.

Sobre esta tarefa

A capacidade em um SVM é calculada como a soma de FlexVols, volumes FlexGroup, FlexClones e volumes FlexCache. Os volumes afetam o cálculo da capacidade mesmo que estejam restritos, offline ou na fila de recuperação após a exclusão. Se você tiver volumes configurados com crescimento automático, o valor máximo de dimensionamento automático do volume será calculado para o tamanho do SVM; sem crescimento automático, o tamanho real do volume será calculado.

A tabela a seguir captura como `autosize-mode` os parâmetros afetam o cálculo da capacidade.

`autosize-mode off`	O parâmetro de tamanho será usado para computação
`autosize-mode grow`	O `max-autosize` parâmetro será usado para computação
`autosize-mode grow-shrink`	O `max-autosize` parâmetro será usado para computação

Antes de começar

- Você deve ser um administrador de cluster para definir um limite de SVM.
- Os limites de storage não podem ser configurados para qualquer SVM que contenha volumes de proteção de dados, volumes em uma relação do SnapMirror ou em uma configuração do MetroCluster.
- Ao migrar um SVM, a fonte SVM não pode ter um limite de storage habilitado. Para concluir a operação de migração, desative o limite de armazenamento na origem e, em seguida, conclua a migração.
- A capacidade do SVM é diferente quotasde . As quotas não podem exceder o tamanho máximo.
- Você não pode definir um limite de storage quando outras operações estiverem em andamento no SVM. Use o `job show vserver` *`svm_name`* comando para ver os trabalhos existentes. Tente executar o comando novamente quando quaisquer trabalhos tiverem sido concluídos.

Impacto na capacidade

Quando você atingir o limite de capacidade, as seguintes operações falharão:

- Criando um LUN, namespace ou volume
- Clonar um LUN, namespace ou volume
- Modificação de um LUN, namespace ou volume
- Aumentar o tamanho de um LUN, namespace ou volume
- Expansão de um LUN, namespace ou volume
- Rehospedando um LUN, namespace ou volume

Defina um limite de capacidade para um novo SVM

System Manager

Passos

1. Selecione **Storage** > **Storage VMs**.
2.  Selecione para criar o SVM.
3. Nomeie o SVM e selecione um **protocolo de acesso**.
4. Em **Storage VM settings**, selecione **Enable maximum capacity limit** (Ativar limite máximo de capacidade).

   Fornecer um tamanho máximo de capacidade para o SVM.

5. Selecione **Guardar**.

CLI

Passos

1. Crie o SVM. Para definir um limite de armazenamento, forneça um `storage-limit` valor. Para definir um alerta de limite para o limite de armazenamento, forneça um valor percentual para `-storage-limit-threshold-alert`o .

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage
   -limit value [GiB|TIB] -storage-limit-threshold-alert percentage [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   Se você não fornecer o valor limite, por padrão, um alerta será acionado quando o SVM tiver 90% de capacidade. Para desativar o alerta de limite, forneça um valor de zero.

2. Confirme se o SVM foi criado com sucesso:

   ```
   vserver show -vserver vserver_name
   ```

3. Se você deseja desativar o limite de armazenamento, modifique o parâmetro SVM com `-storage -limit` zero:

   ```
   vserver modify -vserver vserver_name -storage-limit 0
   ```

Definir ou modificar um limite de capacidade em um SVM existente

Você pode definir um alerta de limite e limite de capacidade em um SVM existente ou desativar um limite de capacidade.

Depois de definir o limite de capacidade, não é possível modificar o limite para um valor inferior à capacidade atualmente alocada.

System Manager

Passos

1. Selecione **Storage** > **Storage VMs**.
2. Selecione o SVM que você deseja modificar. Ao lado do nome do SVM, selecione **Editar**.
3. Para ativar um limite de capacidade, selecione a caixa ao lado de **Ativar limite de capacidade**. Introduza um valor para **capacidade máxima** e um valor percentual para **limiar de alerta**.

   Se desejar desativar o limite de capacidade, desmarque a caixa seguinte **Ativar limite de capacidade**.

4. Selecione **Guardar**.

CLI

Passos

1. No cluster que hospeda o SVM, emita o `vserver modify` comando. Forneça um valor numérico para `-storage-limit` e um valor percentual para `-storage-limit-threshold-alert`.

   ```
   vserver modify -vserver vserver_name -storage-limit value [GiB|TIB]
   -storage-limit-threshold-alert percentage
   ```

   Se você não fornecer o valor limite, terá um alerta padrão com 90% de capacidade. Para desativar o alerta de limite, forneça um valor de zero.

2. Se você deseja desativar o limite de armazenamento, modifique o SVM com `-storage-limit` definido como zero:

   ```
   vserver modify -vserver vserver_name -storage-limit 0
   ```

Atingindo limites de capacidade

Quando você atinge a capacidade máxima ou o limite de alerta, você pode consultar as `vserver.storage.threshold` mensagens EMS ou usar a página **Insights** no System Manager para saber mais sobre possíveis ações. As possíveis resoluções incluem:

- Edição dos limites de capacidade máxima do SVM
- Limpando a fila de recuperação de volumes para liberar espaço
- Eliminar instantâneo para fornecer espaço para o volume

Informações adicionais

- Medições de capacidade no System Manager
- Monitorar a capacidade no System Manager

Use cotas para restringir ou rastrear o uso de recursos

Visão geral do processo de cota

Entenda cotas, regras de cotas e políticas de cotas

As cotas são definidas em regras de cota específicas aos volumes FlexVol. Essas regras de cota são reunidas em uma política de cota para uma máquina virtual de storage (SVM) e ativadas em cada volume no SVM.

Uma regra de cota é sempre específica para um volume. As regras de quota não têm efeito até que as quotas sejam ativadas no volume definido na regra de quota.

Uma política de cota é um conjunto de regras de cota para todos os volumes de um SVM. As políticas de cota não são compartilhadas entre os SVMs. Um SVM pode ter até cinco políticas de cota, o que permite que você tenha cópias de backup de políticas de cota. Uma política de cota é atribuída a um SVM em qualquer momento. Ao inicializar ou redimensionar cotas em um volume, você estará ativando as regras de cota na política de cota atualmente atribuída ao SVM.

Uma cota é a restrição real que o ONTAP impõe ou o rastreamento real que o ONTAP executa. Uma regra de cota sempre resulta em pelo menos uma cota e pode resultar em muitas cotas derivadas adicionais. A lista completa de cotas aplicadas é visível apenas nos relatórios de cotas.

A ativação é o processo de acionar o ONTAP para criar cotas aplicadas a partir do conjunto atual de regras de cota na política de cota atribuída. A ativação ocorre volume a volume. A primeira ativação de cotas em um volume é chamada de inicialização. Ativações subsequentes são chamadas de reinicialização ou redimensionamento, dependendo do escopo das alterações.

Benefícios do uso de cotas

Você pode usar cotas para gerenciar e monitorar o uso de recursos com o FlexVol volumes.

Existem vários benefícios na definição de cotas. Você pode usar as cotas padrão, explícitas, derivadas e de rastreamento para gerenciar o uso do disco da maneira mais eficiente.

Limitar o consumo de recursos

Você pode limitar a quantidade de espaço em disco ou o número de arquivos usados por um usuário ou grupo ou contidos em uma qtree.

Controlar a utilização dos recursos

A quantidade de espaço em disco ou número de arquivos usados por um usuário, grupo ou qtree pode ser rastreada sem impor um limite.

Notifique os usuários

As notificações podem ser geradas quando o uso do recurso atinge níveis específicos. Isso avisa os usuários quando o uso do disco ou do arquivo é muito alto.

Processo de cota

As cotas fornecem uma maneira de restringir ou rastrear o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree. As cotas são aplicadas a um FlexVol volume ou qtree específico.

As quotas podem ser suaves ou difíceis. As cotas flexíveis fazem com que o ONTAP envie uma notificação quando os limites especificados forem excedidos e as cotas rígidas impedem que uma operação de gravação seja bem-sucedida quando os limites especificados forem excedidos.

Quando o ONTAP recebe uma solicitação de um usuário ou grupo de usuários para gravar em um FlexVol volume, ele verifica se as cotas estão ativadas nesse volume para o usuário ou grupo de usuários e determina o seguinte:

- Se o limite rígido será atingido

  Se sim, a operação de gravação falha quando o limite rígido é atingido e a notificação de cota rígida é enviada.

- Se o limite flexível será violado

  Se sim, a operação de gravação é bem-sucedida quando o limite de software é violado e a notificação de cota de software é enviada.

- Se uma operação de gravação não excederá o limite de software

  Se sim, a operação de gravação é bem-sucedida e nenhuma notificação é enviada.

Diferenças entre cotas duras, macias e de limiares

As cotas rígidas impedem operações enquanto as cotas flexíveis acionam notificações.

As cotas rígidas impõem um limite rígido aos recursos do sistema; qualquer operação que resultaria em exceder o limite falha. As seguintes configurações criam cotas rígidas:

- Parâmetro de limite do disco
- Parâmetro limit ficheiros

As cotas flexíveis enviam uma mensagem de aviso quando o uso de recursos atinge um determinado nível, mas não afetam as operações de acesso a dados, para que você possa tomar as medidas apropriadas antes que a cota seja excedida. As configurações a seguir criam cotas flexíveis:

- Limite para o parâmetro limite do disco
- Parâmetro de limite do disco flexível
- Parâmetro de limite de arquivos macios

As cotas de limite e disco flexível permitem que os administradores recebam mais de uma notificação sobre uma cota. Normalmente, os administradores definem o limite de disco para um valor que é apenas ligeiramente menor do que o limite de disco, de modo que o limite forneça um "aviso final" antes de as gravações começarem a falhar.

Acerca das notificações de quota

As notificações de quota são mensagens enviadas para o sistema de gestão de eventos (EMS) e também configuradas como traps SNMP.

As notificações são enviadas em resposta aos seguintes eventos:

- Uma cota difícil é alcançada; em outras palavras, uma tentativa é feita para superá-la
- Uma cota suave é excedida
- Uma quota suave já não é ultrapassada

Os limiares são ligeiramente diferentes de outras quotas moles. Os limites acionam notificações apenas quando são excedidos, não quando já não são excedidos.

As notificações de cota rígida são configuráveis usando o comando de modificação de cota de volume. Você pode desligá-los completamente, e você pode alterar sua frequência, por exemplo, para evitar o envio de mensagens redundantes.

As notificações de cota flexível não são configuráveis porque é improvável que gerem mensagens redundantes e o seu único objetivo é a notificação.

A tabela a seguir lista os eventos que as cotas enviam para o sistema EMS:

Quando isso ocorre…	Este evento é enviado para o EMS…
Um limite rígido é alcançado em uma cota de árvore	`wafl.quota.qtree.exceeded`
Um limite rígido é atingido em uma cota de usuário no volume	`wafl.quota.user.exceeded` (Para um usuário UNIX) `wafl.quota.user.exceeded.win` (para um usuário do Windows)
Um limite rígido é atingido em uma cota de usuário em uma qtree	`wafl.quota.userQtree.exceeded` (Para um usuário UNIX) `wafl.quota.userQtree.exceeded.win` (para um usuário do Windows)
Um limite rígido é atingido em uma cota de grupo no volume	`wafl.quota.group.exceeded`
Um limite rígido é atingido em uma cota de grupo em uma qtree	`wafl.quota.groupQtree.exceeded`
Um limite suave, incluindo um limite, é excedido	`quota.softlimit.exceeded`
Um limite suave já não é excedido	`quota.softlimit.normal`

A tabela a seguir lista os traps SNMP que as cotas geram:

Quando isso ocorre…	Esta trap SNMP é enviada…
Um limite rígido é atingido	QuotaExceeded
Um limite suave, incluindo um limite, é excedido	QuotaExceeded e softQuotaExceeded
Um limite suave já não é excedido	QuotaNormal e softQuotaNormal

As notificações contêm números de ID de qtree em vez de nomes de qtree. Você pode correlacionar nomes de qtree com números de ID usando o `volume qtree show -id` comando.

Cotas e tipos

Cada cota tem um tipo específico. O destino de cota é derivado do tipo e especifica o usuário, grupo ou qtree ao qual os limites de cota são aplicados.

A tabela a seguir lista as metas de cota, os tipos de cotas a que cada meta de cota está associada e como cada meta de cota é representada.

Destino de cota	Tipo de cota	Como o alvo é representado	Notas
utilizador	quota de utilizador	Nome de utilizador UNIX UID UNIX Um arquivo ou diretório cujo UID corresponde ao usuário Nome de utilizador do Windows no formato pré-Windows 2000 Windows SID Um arquivo ou diretório com uma ACL de propriedade do SID do usuário	As cotas de usuário podem ser aplicadas para um volume ou qtree específico.
grupo	cota de grupo	Nome do grupo UNIX GID Um arquivo ou diretório cujo GID corresponde ao grupo	As cotas de grupo podem ser aplicadas para um volume ou qtree específico. O ONTAP não aplica cotas de grupo com base em IDs do Windows.
qtree	cota de árvore	nome de qtree	As cotas de árvore são aplicadas a um volume específico e não afetam qtrees em outros volumes.
""	cota de usuário quotagroup cota de árvore	Aspas duplas (""")	Um alvo de cota de "" denota uma quota *default*. Para cotas padrão, o tipo de cota é determinado pelo valor do campo tipo.

Tipos especiais de cotas

Como funcionam as cotas padrão

Você pode usar cotas padrão para aplicar uma cota a todas as instâncias de um determinado tipo de cota. Por exemplo, uma cota de usuário padrão afeta todos os usuários do sistema para o FlexVol volume ou qtree especificado. Além disso, as cotas padrão permitem que você modifique suas cotas facilmente.

Você pode usar cotas padrão para aplicar automaticamente um limite a um grande conjunto de metas de cota sem ter que criar cotas separadas para cada alvo. Por exemplo, se você quiser limitar a maioria dos usuários a 10 GB de espaço em disco, você pode especificar uma cota de usuário padrão de 10 GB de espaço em disco em vez de criar uma cota para cada usuário. Se você tiver usuários específicos para os quais deseja aplicar um limite diferente, você pode criar cotas explícitas para esses usuários. (Cotas explícitas - cotas com um alvo específico ou lista de metas --substituem cotas padrão.)

Além disso, as cotas padrão permitem que você use o redimensionamento em vez de reinicialização quando você deseja que as alterações de cota entrem em vigor. Por exemplo, se você adicionar uma cota de usuário explícita a um volume que já tenha uma cota de usuário padrão, será possível ativar a nova cota redimensionando.

As cotas padrão podem ser aplicadas a todos os três tipos de destino de cota (usuários, grupos e qtrees).

As cotas padrão não têm necessariamente limites especificados; uma cota padrão pode ser uma cota de rastreamento.

Uma cota é indicada por um destino que é uma string vazia ("""") ou um asterisco (*), dependendo do contexto:

- Quando você cria uma cota usando o `volume quota policy rule create` comando, definir o `-target` parâmetro para uma string vazia ("") cria uma cota padrão.
- No `volume quota policy rule create` comando, o `-qtree` parâmetro especifica o nome da qtree à qual a regra de cota se aplica. Este parâmetro não é aplicável a regras de tipo de árvore. Para regras de tipo de usuário ou grupo no nível de volume, este parâmetro deve conter "".
- Na saída `volume quota policy rule show` do comando, uma cota padrão aparece com uma string vazia ("") como destino.
- Na saída do `volume quota report` comando, uma cota padrão aparece com um asterisco (*) como o especificador de ID e cota.

Exemplo de cota de usuário padrão

A regra de cota a seguir usa uma cota de usuário padrão para aplicar um limite de 50 MB a cada usuário para vol1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -        -
-
```

Se qualquer usuário no sistema inserir um comando que faria com que os dados desse usuário ocupem mais de 50 MB em vol1 (por exemplo, escrevendo em um arquivo de um editor), o comando falhará.

Como você usa cotas explícitas

Você pode usar cotas explícitas para especificar uma cota para um destino de cota específico ou para substituir uma cota padrão para um destino específico.

Uma cota explícita especifica um limite para um determinado usuário, grupo ou qtree. Uma cota explícita substitui qualquer cota padrão que esteja em vigor para o mesmo destino.

Quando você adiciona uma cota de usuário explícita para um usuário que tem uma cota de usuário derivada, você deve usar a mesma configuração de mapeamento de usuário que a cota de usuário padrão. Caso contrário, quando você redimensiona cotas, a cota de usuário explícita é rejeitada porque é considerada uma nova cota.

As cotas explícitas afetam somente as cotas padrão no mesmo nível (volume ou qtree). Por exemplo, uma cota de usuário explícita para uma qtree não afeta a cota de usuário padrão para o volume que contém essa qtree. No entanto, a cota de usuário explícita para a qtree substitui (substitui os limites definidos por) a cota de usuário padrão para essa qtree.

Exemplos de cotas explícitas

As regras de cota a seguir definem uma cota de usuário padrão que limita todos os usuários em vol1 a 50MBMB de espaço. No entanto, um usuário, jsmith, é permitido 80MBMB de espaço, por causa da cota explícita (mostrada em negrito):

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                          User         Disk      Disk    Files    Files
Type   Target    Qtree   Mapping     Limit     Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -        -
-
user   jsmith    ""      off          80MB        -       -        -
-
```

A regra de cota a seguir restringe o usuário especificado, representado por quatro IDs, a 550MB GB de espaço em disco e 10.000 arquivos no volume vol1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                          User         Disk      Disk    Files    Files
Type   Target    Qtree   Mapping     Limit     Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"
                 ""      off         550MB        -   10000        -
-
```

A regra de cota a seguir restringe o grupo eng1 a 150MB GB de espaço em disco e um número ilimitado de arquivos na qtree proj1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
group  eng1      proj1   off         150MB        -       -        -
-
```

A regra de cota a seguir restringe a qtree proj1 no volume vol2 a 750MB GB de espaço em disco e arquivos 75.000:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   proj1     ""      -           750MB        -   75000        -
-
```

Como funcionam as cotas derivadas

Uma cota imposta como resultado de uma cota padrão, em vez de uma cota explícita (uma cota com um alvo específico), é referida como uma cota derivada de _.

O número e a localização das quotas derivadas dependem do tipo de quota:

- Uma cota de árvore padrão em um volume cria cotas de árvore padrão derivadas para cada qtree no volume.
- Uma cota de usuário ou grupo padrão cria uma cota de usuário ou grupo derivada para cada usuário ou

grupo que possua um arquivo no mesmo nível (volume ou qtree).

- Uma cota de usuário ou grupo padrão em um volume cria uma cota de usuário ou grupo padrão derivada em cada qtree que também tem uma cota de árvore.

As configurações - incluindo limites e mapeamento de usuários - de cotas derivadas são as mesmas que as configurações das cotas padrão correspondentes. Por exemplo, uma cota de árvore padrão com um limite de disco de 20 GB em um volume cria cotas de árvore derivadas com limites de disco de 20 GB nos qtrees no volume. Se uma cota padrão for uma cota de rastreamento (sem limites), as cotas derivadas também estão rastreando cotas.

Para ver cotas derivadas, você pode gerar um relatório de cota. No relatório, uma quota de usuário ou grupo derivada é indicada por um especificador de quota que está em branco ou um asterisco (*). Uma cota de árvore derivada, no entanto, tem um especificador de cota; para identificar uma cota de árvore derivada, você deve procurar uma cota de árvore padrão no volume com os mesmos limites.

As quotas explícitas interagem com as quotas derivadas das seguintes formas:

- Cotas derivadas não são criadas se já existir uma cota explícita para o mesmo alvo.
- Se uma cota derivada existir quando você cria uma cota explícita para um destino, você pode ativar a cota explícita redimensionando em vez de ter que executar uma inicialização completa da cota.

Use cotas de rastreamento

Uma cota de rastreamento gera um relatório de uso de disco e arquivo e não limita o uso de recursos. Quando as cotas de rastreamento são usadas, modificar os valores de cota é menos disruptivo porque você pode redimensionar as cotas em vez de desativá-las e ativá-las novamente.

Para criar uma cota de rastreamento, você omita os parâmetros limite de disco e limite de arquivos. Isso diz ao ONTAP para monitorar o uso de disco e arquivos para esse destino nesse nível (volume ou qtree), sem impor limites. As cotas de rastreamento são indicadas na saída `show` de comandos e no relatório de cota com um traço ("-") para todos os limites. O ONTAP cria automaticamente cotas de rastreamento quando você usa a IU do Gerenciador do sistema para criar cotas explícitas (cotas com alvos específicos). Ao usar a CLI, o administrador de armazenamento cria cotas de rastreamento em cima de cotas explícitas.

Você também pode especificar uma cota de rastreamento *padrão*, que se aplica a todas as instâncias do destino. As cotas de rastreamento padrão permitem rastrear o uso de todas as instâncias de um tipo de cota (por exemplo, todos os qtrees ou todos os usuários). Além disso, eles permitem que você use o redimensionamento em vez de reinicialização quando você deseja que as alterações de cota entrem em vigor.

Exemplos

A saída de uma regra de rastreamento mostra cotas de rastreamento em vigor para uma qtree, usuário e grupo, como mostrado no exemplo a seguir para uma regra de rastreamento em nível de volume:

```
Vserver: vs0              Policy: default             Volume: fv1

                                        Soft          Soft
                      User    Disk      Disk   Files  Files
Type  Target   Qtree  Mapping Limit     Limit  Limit  Limit  Threshold
----- -------- ------- ------- ------ ------ ------ ------ ---------
tree  ""       ""      -       -      -      -      -      -
user  ""       ""      off     -      -      -      -      -
group ""       ""      -       -      -      -      -      -
```

Como as cotas são aplicadas

Compreender como as cotas são aplicadas permite configurar as cotas adequadamente e definir os limites esperados.

Sempre que uma tentativa é feita para criar um arquivo ou gravar dados em um arquivo em um FlexVol volume que tenha cotas ativadas, os limites de cota são verificados antes que a operação prossiga. Se a operação exceder o limite de disco ou o limite de arquivos, a operação é impedida.

Os limites de cota são verificados na seguinte ordem:

1. A cota de árvore para essa qtree (essa verificação não é relevante se o arquivo estiver sendo criado ou gravado em qtree0.)
2. A cota de usuário para o usuário que possui o arquivo no volume
3. A cota de grupo para o grupo que possui o arquivo no volume
4. A cota de usuário para o usuário que possui o arquivo na qtree (essa verificação não é relevante se o arquivo estiver sendo criado ou gravado em qtree0).
5. A cota de grupo para o grupo que possui o arquivo na qtree (essa verificação não é relevante se o arquivo estiver sendo criado ou gravado em qtree0).

A quota com o limite mais pequeno pode não ser a que foi ultrapassada primeiro. Por exemplo, se uma cota de usuário para o volume vol1 for de 100 GB e a cota de usuário para a qtree Q2 contida no volume vol1 for de 20 GB, o limite de volume poderá ser atingido primeiro se esse usuário já tiver gravado mais de 80 GB de dados no volume vol1 (mas fora da qtree Q2).

Informações relacionadas

- "Como as cotas são aplicadas ao usuário raiz"
- "Como as cotas são aplicadas a usuários com vários IDs"

Considerações para atribuir políticas de quota

Uma política de cota é um agrupamento das regras de cota para todos os volumes FlexVol de um SVM. Você deve estar ciente de certas considerações ao atribuir as políticas de cota.

- Um SVM tem uma política de cota atribuída a qualquer momento. Quando um SVM é criado, uma política de cota em branco é criada e atribuída ao SVM. Essa política de cota padrão tem o nome "padrão", a menos que um nome diferente seja especificado quando o SVM for criado.

- O SVM pode ter até cinco políticas de cota. Se um SVM tiver cinco políticas de cota, você não poderá criar uma nova política de cota para o SVM até excluir uma política de cota existente.
- Quando você precisa criar uma regra de cota ou alterar regras de cota para uma política de cota, você pode escolher uma das seguintes abordagens:
  - Se você estiver trabalhando em uma política de cota atribuída a um SVM, não será necessário atribuir a política de cota ao SVM.
  - Se estiver trabalhando em uma política de cota não atribuída e atribuindo a diretiva de cota ao SVM, você deverá ter um backup da política de cota para a qual poderá reverter, se necessário.

    Por exemplo, você pode fazer uma cópia da política de cota atribuída, alterar a cópia, atribuir a cópia ao SVM e renomear a política de cota original.
- Você pode renomear uma política de cota mesmo quando ela é atribuída ao SVM.

Como as cotas funcionam com usuários e grupos

Visão geral de como as cotas funcionam com usuários e grupos

Você pode especificar um usuário ou grupo como alvo de uma cota. Há várias diferenças de implementação a considerar ao definir uma cota.

Algumas das diferenças que você precisa estar ciente incluem o seguinte:

- Utilizador ou grupo
- UNIX ou Windows
- Usuários e grupos especiais
- São vários IDs incluídos

Há também maneiras diferentes de especificar IDs para usuários com base em seu ambiente.

Especifique usuários UNIX para cotas

Você pode especificar um usuário UNIX para uma cota em um de vários formatos diferentes.

Os três formatos disponíveis ao especificar um usuário UNIX para uma cota incluem o seguinte:

- O nome de usuário (como jsmith).

  > Você não pode usar um nome de usuário UNIX para especificar uma cota se esse nome incluir uma barra invertida (Isso ocorre porque o ONTAP trata os nomes que contêm esses carateres como nomes do Windows.

- O ID de usuário ou UID (como 20).
- O caminho de um arquivo ou diretório de propriedade desse usuário, para que o UID do arquivo corresponda ao usuário.

Se especificar um nome de ficheiro ou diretório, tem de selecionar um ficheiro ou diretório que durará enquanto a conta de utilizador permanecer no sistema.

Especificar um nome de arquivo ou diretório para o UID não faz com que o ONTAP aplique uma cota a esse arquivo ou diretório.

Especifique usuários do Windows para cotas

Você pode especificar um usuário do Windows para uma cota em um de vários formatos diferentes.

Os três formatos disponíveis ao especificar um usuário do Windows para uma cota incluem o seguinte:

- O nome do Windows no formato pré-Windows 2000.
- O ID de segurança (SID), conforme exibido pelo Windows em forma de texto, como `S-1-5-32-544` .
- O nome de um arquivo ou diretório que tem uma ACL de propriedade do SID desse usuário.

Se especificar um nome de ficheiro ou diretório, tem de selecionar um ficheiro ou diretório que durará enquanto a conta de utilizador permanecer no sistema.

Para que o ONTAP obtenha o SID da ACL, a ACL deve ser válida.

Se o arquivo ou diretório existir em uma qtree de estilo UNIX ou se o sistema de armazenamento usar o modo UNIX para autenticação de usuário, o ONTAP aplica a cota de usuário ao usuário cujo **UID**, não SID, corresponde à do arquivo ou diretório.

Especificar um nome de arquivo ou diretório para identificar um usuário para uma cota não faz com que o ONTAP aplique uma cota a esse arquivo ou diretório.

Como as cotas padrão de usuário e grupo criam cotas derivadas

Quando você cria cotas de usuário ou grupo padrão, as cotas de usuário ou grupo derivadas correspondentes são criadas automaticamente para cada usuário ou grupo que possua arquivos no mesmo nível.

As cotas de usuário e grupo derivadas são criadas das seguintes maneiras:

- Uma cota de usuário padrão em um FlexVol volume cria cotas de usuário derivadas para cada usuário que possui um arquivo em qualquer lugar do volume.
- Uma cota de usuário padrão em uma qtree cria cotas de usuário derivadas para cada usuário que possui um arquivo na qtree.
- Uma cota de grupo padrão em um FlexVol volume cria cotas de grupo derivadas para cada grupo que possui um arquivo em qualquer lugar do volume.
- Uma cota de grupo padrão em uma qtree cria cotas de grupo derivadas para cada grupo que possui um arquivo na qtree.

Se um usuário ou grupo não possuir arquivos no nível de uma cota padrão de usuário ou grupo, as cotas derivadas não serão criadas para o usuário ou grupo. Por exemplo, se uma cota de usuário padrão for criada para a qtree proj1 e o jsmith do usuário possuir arquivos em uma qtree diferente, nenhuma cota de usuário

derivada será criada para o jsmith.

As cotas derivadas têm as mesmas configurações que as cotas padrão, incluindo limites e mapeamento de usuários. Por exemplo, se uma cota de usuário padrão tiver um limite de disco de 50 MB e tiver o mapeamento de usuários ativado, todas as cotas derivadas resultantes também terão um limite de disco de 50 MB e mapeamento de usuários ativados.

No entanto, não existem limites em cotas derivadas para três usuários e grupos especiais. Se os seguintes usuários e grupos possuírem arquivos no nível de uma cota padrão de usuário ou grupo, uma cota derivada é criada com a mesma configuração de mapeamento de usuário que a cota padrão de usuário ou grupo, mas é apenas uma cota de rastreamento (sem limites):

- Usuário raiz UNIX (UID 0)
- Grupo raiz UNIX (GID 0)
- Grupo de administradores do Windows BUILTIN

  Como as cotas para grupos do Windows são rastreadas como cotas de usuário, uma cota derivada para esse grupo é uma cota de usuário derivada de uma cota de usuário padrão, não de uma cota de grupo padrão.

Exemplo de quotas de utilizador derivadas

Se você tiver um volume onde três usuários --root, jsmith e bob—possuem arquivos e criar uma cota de usuário padrão no volume, o ONTAP criará automaticamente três cotas de usuário derivadas. Portanto, depois de reinicializar cotas no volume, quatro novas cotas aparecerão no relatório de cota:

```
cluster1::> volume quota report
  Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *          0B   50MB       0       -   *
vol1               user    root       5B      -       1       -
vol1               user    jsmith    30B   50MB      10       -   *
vol1               user    bob       40B   50MB      15       -   *
4 entries were displayed.
```

A primeira nova linha é a cota de usuário padrão que você criou, que é identificável pelo asterisco (*) como ID. As outras novas linhas são as quotas de utilizador derivadas. As cotas derivadas para jsmith e bob têm o mesmo limite de disco de 50 MB que a cota padrão. A cota derivada para o usuário raiz é uma cota de rastreamento sem limites.

Como as cotas são aplicadas ao usuário raiz

O usuário root (UID-0) em clientes UNIX está sujeito a cotas de árvore, mas não a cotas de usuário ou grupo. Isso permite que o usuário root tome ações em nome de outros usuários que, de outra forma, seriam impedidas por uma cota.

Quando o usuário root realiza uma alteração de propriedade de arquivo ou diretório ou outra operação (como o comando UNIX `chown`) em nome de um usuário com menos Privileges, o ONTAP verifica as cotas com base no novo proprietário, mas não relata erros ou interrompe a operação, mesmo que as restrições de cota rígida do novo proprietário sejam excedidas. Isso pode ser útil quando uma ação administrativa, como a recuperação de dados perdidos, resulta em exceder temporariamente as cotas.

Depois que a transferência de propriedade é realizada, no entanto, um sistema cliente irá relatar um erro de espaço em disco se o usuário tentar alocar mais espaço em disco enquanto a cota ainda é excedida.

Informações relacionadas

- "Como as cotas são aplicadas"
- "Como as cotas são aplicadas a usuários com vários IDs"

Como as cotas funcionam com grupos especiais do Windows

Existem vários grupos especiais do Windows que processam cotas de forma diferente dos outros grupos do Windows. Você deve entender como as cotas são aplicadas para esses grupos especiais.

O ONTAP não suporta cotas de grupo com base em IDs de grupo do Windows. Se você especificar um ID de grupo do Windows como destino de cota, a cota será considerada uma cota de usuário.

Todos

Quando o destino da cota é o grupo todos, um arquivo com uma ACL mostrando que o proprietário é todos é contado sob o SID para todos.

CRIAR/Administradores

Quando o alvo de cota é o grupo BUILTIN/Administradores, a entrada é considerada uma cota de usuário e é usada apenas para rastreamento. Não é possível impor restrições a BUILTIN/Administradores. Se um membro do BUILTIN/Administradores criar um arquivo, o arquivo é de propriedade de BUILTIN/Administradores e é contado sob o SID para BUILTIN/Administradores (não o SID pessoal do usuário).

Como as cotas são aplicadas a usuários com vários IDs

Um usuário pode ser representado por vários IDs. Você pode definir uma única cota de usuário para tal usuário especificando uma lista de IDs como o destino da cota. Um arquivo de propriedade de qualquer um desses IDs está sujeito à restrição da cota de usuário.

Suponha que um usuário tenha o UID UNIX `20` e os IDs do Windows `corp\john_smith` e `engineering\jsmith`. Para esse usuário, você pode especificar uma cota em que o destino da cota é uma lista de UID e IDs do Windows. Quando esse usuário grava no sistema de armazenamento, a cota especificada se aplica, independentemente de a gravação ter origem em UID `20`, `corp\john_smith` ou `engineering\jsmith`.

Observe que regras de cota separadas são consideradas alvos separados, mesmo que os IDs pertençam ao mesmo usuário. Por exemplo, para o mesmo usuário, você pode especificar uma cota que limita UID `20` a 1GBMB de espaço em disco e outra cota que limita corp john_smith a 2GBMB de espaço em disco, mesmo

que ambos os IDs representem o mesmo usuário. O ONTAP aplica cotas a UID `20` e `corp\john_smith` separadamente. Nesse caso, não são aplicados limites ao `engineering\jsmith`, mesmo que os limites sejam aplicados aos outros IDs usados pelo mesmo usuário.

Informações relacionadas

- "Como as cotas são aplicadas"
- "Como as cotas são aplicadas ao usuário raiz"

Como o ONTAP determina as IDs de usuário em um ambiente misto

Se você tiver usuários acessando o armazenamento do ONTAP a partir de clientes Windows e UNIX, a segurança do Windows e UNIX será usada para determinar a propriedade do arquivo. Vários fatores determinam se o ONTAP usa um ID UNIX ou Windows ao aplicar cotas de usuário.

Se o estilo de segurança da qtree ou FlexVol volume que contém o arquivo for apenas NTFS ou apenas UNIX, o estilo de segurança determina o tipo de ID usado ao aplicar cotas de usuário. Para qtrees com o estilo de segurança misto, o tipo de ID usado é determinado se o arquivo tem uma ACL.

A tabela a seguir resume qual tipo de ID é usado.

Estilo de segurança	ACL	Sem ACL
UNIX	ID UNIX	ID UNIX
Misto	ID do Windows	ID UNIX
NTFS	ID do Windows	ID do Windows

Como as cotas funcionam com vários usuários

Quando você coloca vários usuários no mesmo destino de cota, os limites definidos pela cota não são aplicados a cada usuário individual. Em vez disso, os limites de cota são compartilhados entre todos os usuários no destino de cota.

Ao contrário dos comandos para gerenciar objetos, como volumes e qtrees, você não pode renomear um destino de cota, incluindo uma cota multiusuário. Isso significa que depois que uma cota de vários usuários é definida, você não pode modificar os usuários no destino de cota e não pode adicionar usuários a um destino ou remover usuários de um destino. Se você quiser adicionar ou remover um usuário de uma cota de vários usuários, a cota que contém esse usuário deve ser excluída e uma nova regra de cota com o conjunto de usuários no destino definido.

> Se você combinar cotas de usuário separadas em uma cota de vários usuários, poderá ativar a alteração reredimensionando cotas. No entanto, se você quiser remover usuários de um destino de cota com vários usuários ou adicionar usuários a um destino que já tenha vários usuários, será necessário reinicializar cotas antes que a alteração entre em vigor.

Exemplo de mais de um usuário em uma regra de cota

No exemplo a seguir, há dois usuários listados na entrada de cota. Os dois usuários podem usar até 80MBMB de espaço combinado. Se um usa 75MB, então o outro pode usar apenas 5MB.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                    Soft             Soft
                              User         Disk     Disk   Files    Files
Type   Target         Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------       ------- -------  --------  -------  ------  -------
---------
user   "jsmith,chen"  ""      off          80MB        -       -        -
-
```

Vinculação de nomes UNIX e Windows para cotas

Em um ambiente misto, os usuários podem fazer login como usuários do Windows ou usuários UNIX. Você pode configurar cotas para reconhecer que o ID UNIX de um usuário e o ID do Windows representam o mesmo usuário.

As cotas para o nome de usuário do Windows são mapeadas para um nome de usuário UNIX, ou vice-versa, quando ambas as condições a seguir são atendidas:

- O `user-mapping` parâmetro é definido como "On" (ligado) na regra de quota para o utilizador.
- Os nomes de usuário foram mapeados com os `vserver name-mapping` comandos.

Quando um nome UNIX e Windows são mapeados juntos, eles são tratados como a mesma pessoa para determinar o uso da cota.

Como as cotas de árvores funcionam

Visão geral de como as cotas de árvores funcionam

Você pode criar uma cota com uma qtree como destino para limitar o tamanho da qtree de destino. Essas cotas também são chamadas de *cotas de árvores*.

> Você também pode criar cotas de usuário e grupo para uma qtree específica. Além disso, as cotas para um FlexVol volume às vezes são herdadas pelos qtrees contidos por esse volume.

Quando você aplica uma cota a uma qtree, o resultado é semelhante a uma partição de disco, exceto que você pode alterar o tamanho máximo da qtree a qualquer momento alterando a cota. Ao aplicar uma cota de árvore, o ONTAP limita o espaço em disco e o número de arquivos na qtree, independentemente de seus proprietários. Nenhum usuário, incluindo root e membros do grupo BUILTIN/Administradores, pode gravar na qtree se a operação de gravação fizer com que a cota da árvore seja excedida.

O tamanho da cota não garante qualquer quantidade específica de espaço disponível. O tamanho da cota

pode ser maior do que a quantidade de espaço livre disponível para a qtree. Você pode usar o `volume quota report` comando para determinar a verdadeira quantidade de espaço disponível na qtree.

Como as cotas de usuário e grupo funcionam com qtrees

As cotas de árvore limitam o tamanho geral da qtree. Para impedir que usuários ou grupos individuais consumam toda a qtree, você especifica uma cota de usuário ou grupo para essa qtree.

Exemplo de cota de usuário em uma qtree

Suponha que você tenha as seguintes regras de cota:

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           50MB        -       -        -
45MB
user   jsmith    ""      off           80MB        -       -        -
75MB
```

Você percebe que um determinado usuário, kjones, está ocupando muito espaço em uma qtree crítica, proj1, que reside no vol1. Você pode restringir o espaço desse usuário adicionando a seguinte regra de cota:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -        -
45MB
user   jsmith    ""      off          80MB        -       -        -
75MB
user   kjones    proj1   off          20MB        -       -        -
15MB
```

Como as cotas de árvore padrão em um FlexVol volume criam cotas de árvore derivadas

Quando você cria uma cota de árvore padrão em um FlexVol volume, as cotas de árvore derivadas correspondentes são criadas automaticamente para cada qtree nesse volume.

Essas cotas de árvore derivadas têm os mesmos limites que a cota de árvore padrão. Se não existirem quotas adicionais, os limites têm os seguintes efeitos:

- Os usuários podem usar tanto espaço em uma qtree como eles são alocados para todo o volume (desde que eles não excedessem o limite para o volume usando espaço na raiz ou em outra qtree).
- Cada um dos qtrees pode crescer para consumir todo o volume.

A existência de uma cota de árvore padrão em um volume continua a afetar todos os novos qtrees que são adicionados ao volume. Cada vez que uma nova qtree é criada, uma cota de árvore derivada também é criada.

Como todas as cotas derivadas, as cotas de árvore derivadas exibem os seguintes comportamentos:

- São criados somente se o alvo ainda não tiver uma cota explícita.
- Aparecem nos relatórios de cota, mas não aparecem quando você mostra regras de cota com o `volume quota policy rule show` comando.

Exemplo de cotas de árvores derivadas

Você tem um volume com três qtrees (proj1, proj2 e proj3) e a única cota de árvore é uma cota explícita na qtree proj1 que limita seu tamanho de disco a 10 GB. Se você criar uma cota de árvore padrão no volume e reinicializar cotas no volume, o relatório de cota agora contém quatro cotas de árvore:

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     tree    1           0B   10GB       1       -   proj1
vol1               tree    *           0B   20GB       0       -   *
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj3     tree    3           0B   20GB       1       -   proj3
...
```

A primeira linha mostra a cota explícita original na qtree proj1. Esta quota permanece inalterada.

A segunda linha mostra a nova cota de árvore padrão no volume. O especificador de cota asterisco (*) indica que é uma cota padrão. Essa cota é resultado da regra de cota que você criou.

As duas últimas linhas mostram novas cotas de árvores derivadas para os qtrees proj2 e proj3. O ONTAP criou automaticamente essas cotas como resultado da cota de árvore padrão no volume. Essas cotas de árvore derivadas têm o mesmo limite de disco de 20 GB que a cota de árvore padrão no volume. O ONTAP não criou uma cota de árvore derivada para a qtree proj1 porque a qtree proj1 já tinha uma cota explícita.

Como as cotas de usuário padrão em um FlexVol volume afetam as cotas para qtrees nesse volume

Se uma cota de usuário padrão for definida para um FlexVol volume, uma cota de usuário padrão será criada automaticamente para cada qtree contido nesse volume para o qual existe uma cota de árvore explícita ou derivada.

Se uma cota de usuário padrão na qtree já existir, ela permanecerá inalterada quando a cota de usuário padrão no volume for criada.

As cotas de usuário padrão criadas automaticamente no qtrees têm os mesmos limites que a cota de usuário padrão criada para o volume.

Uma cota de usuário explícita para uma qtree substitui (substitui os limites aplicados) a cota de usuário padrão criada automaticamente, da mesma forma que substitui uma cota de usuário padrão nessa qtree criada por um administrador.

Como as alterações de qtree afetam as cotas

Ao excluir, renomear ou alterar o estilo de segurança de uma qtree, as cotas aplicadas pelo ONTAP podem mudar, dependendo das cotas atuais sendo aplicadas.

Exclusões de Qtree e quotas de árvore

Quando você exclui uma qtree, todas as cotas aplicáveis a essa qtree, explícitas ou derivadas, não são mais aplicadas pelo ONTAP.

Se as regras de cota persistem depende de onde você exclui a qtree:

- Se você excluir uma qtree usando o ONTAP, as regras de cota para essa qtree serão automaticamente

excluídas, incluindo regras de cota de árvore e quaisquer regras de cota de usuário e grupo configuradas para essa qtree.

- Se você excluir uma qtree usando seu cliente CIFS ou NFS, será necessário excluir quaisquer regras de cota para essa qtree para evitar erros ao reinicializar cotas. Se você criar uma nova qtree com o mesmo nome que o que você excluiu, as regras de cota existentes não serão aplicadas à nova qtree até que você reinicialize cotas.

Como renomear uma qtree afeta as cotas

Quando você renomear uma qtree usando o ONTAP, as regras de cota para essa qtree são atualizadas automaticamente. Se você renomear uma qtree usando seu cliente CIFS ou NFS, será necessário atualizar as regras de cota para essa qtree.

> Se você renomear uma qtree usando seu cliente CIFS ou NFS e não atualizar as regras de cota para essa qtree com o novo nome antes de reinicializar as cotas, as cotas não serão aplicadas à qtree. Cotas explícitas para a qtree, incluindo cotas de árvore e cotas de usuário ou grupo para a qtree, podem ser convertidas em cotas derivadas.

Estilos de segurança Qtree e cotas de usuário

Você pode aplicar listas de controle de acesso (ACLs) em qtrees usando estilos de segurança NTFS ou mistos, mas não usando o estilo de segurança UNIX. Alterar o estilo de segurança de uma qtree pode afetar a forma como as cotas são calculadas. Você deve sempre reinicializar cotas depois de alterar o estilo de segurança de uma qtree.

Se você alterar o estilo de segurança de uma qtree de NTFS ou misto para UNIX, quaisquer ACLs em arquivos nessa qtree serão ignoradas e o uso do arquivo será cobrado contra as IDs de usuário UNIX.

Se você alterar o estilo de segurança de uma qtree de UNIX para Misto ou NTFS, as ACLs ocultas anteriormente ficam visíveis. Além disso, quaisquer ACLs que foram ignoradas se tornam efetivas novamente e as informações do usuário NFS são ignoradas. Se nenhuma ACL existisse antes, as informações NFS continuarão a ser usadas no cálculo da cota.

> Para garantir que os usos de cota para usuários UNIX e Windows sejam calculados corretamente depois que você alterar o estilo de segurança de uma qtree, é necessário reinicializar as cotas para o volume que contém essa qtree.

Exemplo

O exemplo a seguir mostra como uma alteração no estilo de segurança de uma qtree resulta em um usuário diferente sendo cobrado pelo uso de um arquivo na qtree em particular.

Suponha que a segurança NTFS esteja em vigor na qtree A e uma ACL dê ao usuário do Windows A `corp\joe` propriedade de um arquivo 5MB. O usuário `corp\joe` é carregado com 5MB GB de uso de espaço em disco para uma

Agora você altera o estilo de segurança da qtree A de NTFS para UNIX. Depois que as cotas forem reinicializadas, o usuário do Windows `corp\joe` não será mais cobrado por esse arquivo; em vez disso, o usuário UNIX correspondente ao UID do arquivo será cobrado pelo arquivo. O UID pode ser um usuário UNIX mapeado para `corp\joe` ou para o usuário raiz.

Como as cotas são ativadas

Visão geral de como as cotas são ativadas

Novas quotas e alterações às quotas existentes devem ser ativadas para serem efetivas. A ativação é efetuada ao nível do volume. Saber como funciona a ativação de cotas pode ajudá-lo a gerenciar suas cotas com menos interrupções.

As cotas são ativadas por *inicializando* (ativando-as) ou por *redimensionamento*. Desativar cotas e ativá-las novamente é chamado de reinicializing.

A duração do processo de ativação e o seu impactos na aplicação da quota depende do tipo de ativação:

- O processo de inicialização envolve duas partes: Uma `quota on` tarefa e uma varredura de cota de todo o sistema de arquivos do volume. A digitalização começa após `quota on` a conclusão do trabalho com êxito. A verificação de quota pode demorar algum tempo; quanto mais ficheiros tiver o volume, mais tempo demora. Até que a digitalização esteja concluída, a ativação da quota não está concluída e as quotas não são aplicadas.
- O processo de redimensionamento envolve apenas um `quota resize` trabalho. O redimensionamento demora menos tempo do que uma inicialização de quota porque não envolve uma verificação de quota. Durante um processo de redimensionamento, as cotas continuam a ser aplicadas.

Por predefinição, os `quota on` trabalhos e `quota resize` são executados em segundo plano, o que permite utilizar outros comandos ao mesmo tempo.

Erros e avisos do processo de ativação são enviados para o sistema de gerenciamento de eventos. Se você usar o `-foreground` parâmetro com os `volume quota on` comandos ou `volume quota resize`, o comando não retornará até que a tarefa esteja concluída; isso será útil se você estiver reinicializando a partir de um script. Para exibir erros e avisos mais tarde, você pode usar o `volume quota show` comando com o `-instance` parâmetro.

A ativação da cota persiste entre paradas e reinicializações. O processo de ativação da cota não afeta a disponibilidade dos dados do sistema de armazenamento.

Entenda quando usar o redimensionamento

O redimensionamento de cotas é um recurso útil do ONTAP. E como o redimensionamento é mais rápido do que a inicialização da cota, você deve usar o redimensionamento sempre que possível. No entanto, existem algumas restrições que você precisa estar ciente.

O redimensionamento só funciona para certos tipos de alterações de cota. Você pode redimensionar cotas ao fazer os seguintes tipos de alterações nas regras de cota:

- Alterar uma cota existente.

  Por exemplo, alterando os limites de uma cota existente.

- Adicionar uma cota para um destino de cota para o qual existe uma cota padrão ou uma cota de rastreamento padrão.
- Exclusão de uma cota para a qual uma cota padrão ou entrada de cota de rastreamento padrão é especificada.
- Combinando cotas de usuário separadas em uma cota de multiusuário.

Depois de fazer alterações extensas de cotas, você deve executar uma reinicialização completa para garantir que todas as alterações entrem em vigor.

Se você tentar redimensionar e nem todas as alterações de cota podem ser incorporadas usando uma operação de redimensionamento, o ONTAP emite um aviso. Você pode determinar no relatório de cota se o sistema de storage está rastreando o uso do disco para um determinado usuário, grupo ou qtree. Se você vir uma cota no relatório de cota, isso significa que o sistema de armazenamento está rastreando o espaço em disco e o número de arquivos de propriedade do destino de cota.

Exemplo de alterações de cotas que podem ser efetivadas pelo redimensionamento

Algumas alterações de regra de cota podem ser efetivadas pelo redimensionamento. Considere as seguintes cotas:

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----             ----  ----- ----- ----- -----
*             user@/vol/vol2    50M   15K
*             group@/vol/vol2  750M   85K
*             tree@/vol/vol2     -     -
jdoe          user@/vol/vol2/  100M   75K
kbuck         user@/vol/vol2/  100M   75K
```

Suponha que você faça as seguintes alterações:

- Aumente o número de arquivos para o destino de usuário padrão.
- Adicione uma nova cota de usuário para um novo usuário, o boris, que precisa de mais limite de disco do que a cota de usuário padrão.
- Exclua a entrada de cota explícita do usuário kbuck; o novo usuário agora precisa apenas dos limites de cota padrão.

Estas alterações resultam nas seguintes quotas:

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----             ----  ----- ----- ----- -----
*             user@/vol/vol2    50M   25K
*             group@/vol/vol2  750M   85K
*             tree@/vol/vol2     -     -
jdoe          user@/vol/vol2/  100M   75K
boris         user@/vol/vol2/  100M   75K
```

O redimensionamento ativa todas essas alterações; uma reinicialização total da cota não é necessária.

Quando é necessária uma reinicialização total da quota

Embora o redimensionamento de cotas seja mais rápido, você deve fazer uma reinicialização total da cota se fizer certas alterações pequenas ou extensas em suas

cotas.

É necessária uma reinicialização total da quota nas seguintes circunstâncias:

- Você cria uma cota para um destino que não tinha uma cota anteriormente (nem uma cota explícita nem uma derivada de uma cota padrão).
- Você altera o estilo de segurança de uma qtree de UNIX para misto ou NTFS.
- Você altera o estilo de segurança de uma qtree de misto ou NTFS para UNIX.
- Você remove usuários de um destino de cota com vários usuários ou adiciona usuários a um destino que já tenha vários usuários.
- Você faz mudanças extensas em suas cotas.

Exemplo de alterações de cotas que exigem inicialização

Suponha que você tenha um volume que contenha três qtrees e as únicas cotas no volume são três cotas de árvore explícitas. Você decide fazer as seguintes alterações:

- Adicione uma nova qtree e crie uma nova cota de árvore para ela.
- Adicione uma cota de usuário padrão para o volume.

Ambas as alterações requerem uma inicialização completa da quota. O redimensionamento não torna as cotas efetivas.

Como você pode exibir informações de cota

Visão geral da exibição de informações de cota

Você pode usar relatórios de cota para exibir detalhes como a configuração de regras e políticas de cota, cotas aplicadas e configuradas e erros que ocorreram durante o redimensionamento e reinicialização de cotas.

A visualização de informações de cota é útil em situações como as seguintes:

- Configurando cotas, por exemplo, para configurar cotas e verificar as configurações
- Responder a notificações de que o espaço em disco ou os limites de arquivo serão alcançados em breve ou que foram alcançados
- Respondendo a solicitações de mais espaço

Veja quais cotas estão em vigor usando o relatório de cotas

Por causa das várias maneiras pelas quais as cotas interagem, mais cotas estão em vigor do que apenas as que você criou explicitamente. Para ver quais cotas estão em vigor, você pode visualizar o relatório de cota.

Os exemplos a seguir mostram relatórios de cotas para diferentes tipos de cotas aplicadas em um FlexVol volume vol1 e uma qtree Q1 contida nesse volume:

Exemplo sem cotas de usuário especificadas para a qtree

Neste exemplo, há uma qtree, Q1, que é contido pelo volume vol1. O administrador criou três cotas:

- Um limite de cota de árvore padrão em vol1 de 400MB

- Um limite de cota de usuário padrão em vol1 de 100MB
- Um limite de quota de utilizador explícito em vol1 de 200MB para o utilizador jsmith

As regras de quota para estas quotas são semelhantes ao seguinte exemplo:

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                  Soft             Soft
                          User          Disk      Disk    Files    Files
Type   Target    Qtree    Mapping      Limit     Limit    Limit    Limit
Threshold
-----  --------  -------  -------  --------  -------  ------  -------
---------
tree   ""        ""       -           400MB         -       -        -
-
user   ""        ""       off         100MB         -       -        -
-
user   jsmith    ""       off         200MB         -       -        -
-
```

O relatório de quota para estas quotas é semelhante ao seguinte exemplo:

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith    150B  200MB       7       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     q1         user   *           0B  100MB       0       -
vol1     q1         user   jsmith      0B  100MB       5       -
vol1     -          user   root        0B    0MB       1       -
vol1     q1         user   root        0B    0MB       8       -
```

As três primeiras linhas do relatório de cota exibem as três cotas especificadas pelo administrador. Como duas dessas cotas são cotas padrão, o ONTAP cria automaticamente cotas derivadas.

A quarta linha exibe a cota de árvore derivada da cota de árvore padrão para cada qtree em vol1 (neste exemplo, apenas Q1).

A quinta linha exibe a cota de usuário padrão criada para a qtree como resultado da existência da cota de

usuário padrão no volume e na cota de qtree.

A sexta linha exibe a cota de usuário derivada que é criada para jsmith na qtree porque há uma cota de usuário padrão para a qtree (linha 5) e o jsmith do usuário possui arquivos nessa qtree. Observe que o limite aplicado ao jsmith do usuário na qtree Q1 não é determinado pelo limite explícito de cota de usuário (200MB). Isso ocorre porque o limite explícito de cota de usuário está no volume, portanto, não afeta os limites para a qtree. Em vez disso, o limite de cota de usuário derivado para a qtree é determinado pela cota de usuário padrão para a qtree (100MB).

As duas últimas linhas exibem mais cotas de usuário que são derivadas das cotas de usuário padrão no volume e na qtree. Uma cota de usuário derivada foi criada para o usuário raiz no volume e na qtree porque o usuário raiz possuía arquivos no volume e na qtree. Como o usuário raiz recebe tratamento especial em termos de cotas, suas cotas derivadas estão rastreando somente cotas.

Exemplo com cotas de usuário especificadas para a qtree

Este exemplo é semelhante ao anterior, exceto que o administrador adicionou duas cotas na qtree.

Ainda há um volume, vol1 e uma qtree, Q1. O administrador criou as seguintes cotas:

- Um limite de cota de árvore padrão em vol1 de 400MB
- Um limite de cota de usuário padrão em vol1 de 100MB
- Um limite de quota de utilizador explícito em vol1 para o utilizador jsmith de 200MB
- Um limite de cota de usuário padrão na qtree Q1 de 50MB
- Um limite de cota de usuário explícito na qtree Q1 para o jsmith de usuário de 75MB

As regras de quota para estas quotas são assim:

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   ""        ""      -           400MB        -       -        -
-
user   ""        ""      off         100MB        -       -        -
-
user   ""        q1      off          50MB        -       -        -
-
user   jsmith    ""      off         200MB        -       -        -
-
user   jsmith    q1      off          75MB        -       -        -
-
```

O relatório de quotas para estas quotas é assim:

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith   2000B  200MB       7       -   jsmith
vol1     q1         user   *           0B   50MB       0       -   *
vol1     q1         user   jsmith      0B   75MB       5       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     -          user   root        0B    0MB       2       -
vol1     q1         user   root        0B    0MB       1       -
```

As primeiras cinco linhas do relatório de cota exibem as cinco cotas criadas pelo administrador. Como algumas dessas cotas são cotas padrão, o ONTAP cria automaticamente cotas derivadas.

A sexta linha exibe a cota de árvore derivada da cota de árvore padrão para cada qtree em vol1 (neste exemplo, apenas Q1).

As duas últimas linhas exibem as cotas de usuário que são derivadas das cotas de usuário padrão no volume e na qtree. Uma cota de usuário derivada foi criada para o usuário raiz no volume e na qtree porque o usuário raiz possuía arquivos no volume e na qtree. Como o usuário raiz recebe tratamento especial em termos de cotas, suas cotas derivadas estão rastreando somente cotas.

Não foram criadas outras quotas de incumprimento ou quotas derivadas pelas seguintes razões:

- Uma cota de usuário derivada não foi criada para o usuário jsmith, embora o usuário possua arquivos no volume e na qtree, porque o usuário já tem cotas explícitas em ambos os níveis.
- Não foram criadas quotas de utilizador derivadas para outros utilizadores porque nenhum outro utilizador possui ficheiros no volume ou na qtree.
- A cota de usuário padrão no volume não criou uma cota de usuário padrão na qtree porque a qtree já tinha uma cota de usuário padrão.

Por que as cotas aplicadas diferem das cotas configuradas

As cotas aplicadas diferem das cotas configuradas porque as cotas derivadas são aplicadas sem serem configuradas, mas as cotas configuradas são aplicadas somente após serem inicializadas com êxito. A compreensão dessas diferenças pode ajudá-lo a comparar as cotas aplicadas mostradas nos relatórios de cotas com as cotas configuradas.

As cotas aplicadas, que aparecem nos relatórios de cotas, podem diferir das regras de cota configuradas pelas seguintes razões:

- Cotas derivadas são aplicadas sem serem configuradas como regras de cota. O ONTAP cria cotas

derivadas automaticamente em resposta às cotas padrão.

- As cotas podem não ter sido reinicializadas em um volume após as regras de cota terem sido configuradas.
- Podem ter ocorrido erros quando as cotas foram inicializadas em um volume.

Use o relatório de cota para determinar qual limite de cotas grava em um arquivo específico

Você pode usar o comando de relatório de cota de volume com um caminho de arquivo específico para determinar quais limites de cota afetam as operações de gravação em um arquivo. Isso pode ajudá-lo a entender qual cota está impedindo uma operação de gravação.

Passos

1. Use o comando volume quota report com o parâmetro -path.

Exemplo de mostrar cotas que afetam um arquivo específico

O exemplo a seguir mostra o comando e a saída para determinar quais cotas estão em vigor para gravações no arquivo file1, que reside no qtree Q1 no FlexVol volume vol2:

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     q1        tree    jsmith     1MB  100MB       2   10000   q1
vol2     q1        group   eng        1MB  700MB       2   70000
vol2               group   eng        1MB  700MB       6   70000   *
vol2               user    corp\jsmith
                                      1MB   50MB       1       -   *
vol2     q1        user    corp\jsmith
                                      1MB   50MB       1       -
5 entries were displayed.
```

Comandos para exibir informações sobre cotas

Você pode usar comandos para exibir um relatório de cota contendo cotas aplicadas e uso de recursos, exibir informações sobre o estado e erros da cota ou sobre políticas de cota e regras de cota.

Você pode executar os seguintes comandos apenas no FlexVol volumes.

Se você quiser…	Use este comando…
Exibir informações sobre cotas aplicadas	`volume quota report`
Exibir o uso de recursos (espaço em disco e número de arquivos) de alvos de cota	`volume quota report`
Determine quais limites de cota são afetados quando uma gravação em um arquivo é permitida	`volume quota report` com o `-path` parâmetro
Exiba o estado da cota, como `on` , `off` e `initializing`	`volume quota show`
Exibir informações sobre o Registro de mensagens de cota	`volume quota show` com o `-logmsg` parâmetro
Veja erros que ocorrem durante a inicialização e redimensionamento da cota	`volume quota show` com o `-instance` parâmetro
Exibir informações sobre políticas de cota	`volume quota policy show`
Exibir informações sobre regras de cota	`volume quota policy rule show`
Exibir o nome da política de cota atribuída a uma máquina virtual de storage (SVM, anteriormente conhecido como SVM)	`vserver show` com o `-instance` parâmetro

Consulte a página de manual de cada comando para obter mais informações.

Quando usar os comandos show de regra de diretiva de cota de volume e relatório de cota de volume

Embora ambos os comandos mostrem informações sobre cotas, o `volume quota policy rule show` exibe rapidamente regras de cota configuradas enquanto o `volume quota report` comando, que consome mais tempo e recursos, exibe cotas aplicadas e uso de recursos.

O `volume quota policy rule show` comando é útil para os seguintes propósitos:

- Verifique a configuração das regras de quota antes de as ativar

  Este comando exibe todas as regras de cota configuradas, independentemente de as cotas terem sido inicializadas ou redimensionadas.

- Visualize rapidamente as regras de cota sem afetar os recursos do sistema

  Como ele não exibe o uso do disco e do arquivo, esse comando não é tão intensivo em recursos quanto um relatório de cota.

- Exiba as regras de cota em uma política de cota que não esteja atribuída ao SVM.

O `volume quota report` comando é útil para os seguintes propósitos:

- Veja cotas aplicadas, incluindo cotas derivadas
- Visualize o espaço em disco e o número de arquivos usados por cada cota em vigor, incluindo alvos afetados por cotas derivadas

  (Para cotas padrão, o uso aparece como "0" porque o uso é rastreado contra a cota derivada resultante.)

- Determine quais limites de cota afetam quando uma gravação em um arquivo será permitida

  Adicione o `-path` parâmetro ao `volume quota report` comando.

> O relatório de cota é uma operação intensiva em recursos. Se você executá-lo em muitos volumes do FlexVol no cluster, poderá levar muito tempo para ser concluído. Uma maneira mais eficiente seria visualizar o relatório de cotas de um determinado volume em um SVM.

Diferença no uso do espaço exibido por um relatório de cota e um cliente UNIX

Visão geral da diferença no uso de espaço exibida por um relatório de cota e um cliente UNIX

O valor do espaço em disco usado exibido em um relatório de cota para um FlexVol volume ou qtree pode ser diferente do valor exibido por um cliente UNIX para o mesmo volume ou qtree. A diferença nesses valores é devido aos diferentes métodos seguidos pelo relatório de cota e pelos comandos UNIX para calcular os blocos de dados no volume ou qtree.

Por exemplo, se um volume contiver um arquivo que tenha blocos de dados vazios (para os quais os dados não são gravados), o relatório de cota para o volume não contará os blocos de dados vazios enquanto relata o uso do espaço. No entanto, quando o volume é montado em um cliente UNIX e o arquivo é mostrado como a saída `ls` do comando, os blocos de dados vazios também são incluídos no uso do espaço. Portanto, o `ls` comando exibe um tamanho de arquivo maior quando comparado ao uso de espaço exibido pelo relatório de cota.

Da mesma forma, os valores de uso de espaço mostrados em um relatório de cota também podem diferir dos valores mostrados como resultado de comandos UNIX `df` como e `du`.

Como um relatório de quota é responsável pelo espaço em disco e pelo uso de arquivos

O número de arquivos usados e a quantidade de espaço em disco especificada em um relatório de cota para um FlexVol volume ou uma qtree dependem da contagem dos blocos de dados usados correspondentes a cada inode no volume ou na qtree.

A contagem de blocos inclui blocos diretos e indiretos usados para arquivos regulares e de fluxo. Os blocos usados para diretórios, listas de controle de acesso (ACLs), diretórios de fluxo e metafiles não são contabilizados no relatório de cota. No caso de arquivos esparsos UNIX, blocos de dados vazios não são incluídos no relatório de cota.

O subsistema quota foi projetado para considerar e incluir apenas aspetos controláveis pelo usuário do sistema de arquivos. Diretórios, ACLs e espaço de snapshot são todos exemplos de espaço excluído dos cálculos de cotas. As cotas são usadas para impor limites, não garantias, e elas só operam no sistema de

arquivos ativo. A contagem de cotas não conta certas construções de sistema de arquivos, nem conta para eficiência de storage (como compactação ou deduplicação).

Disparidade entre o comando ls e o relatório de cota para uso de espaço

Quando você usa o `ls` comando para exibir o conteúdo de um FlexVol volume montado em um cliente UNIX, os tamanhos de arquivo exibidos na saída podem diferir do uso de espaço exibido no relatório de cota para o volume, dependendo do tipo de blocos de dados para o arquivo.

A saída do `ls` comando exibe apenas o tamanho de um arquivo e não inclui blocos indiretos usados pelo arquivo. Quaisquer blocos vazios do arquivo também são incluídos na saída do comando.

Portanto, se um arquivo não tiver blocos vazios, o tamanho exibido pelo `ls` comando pode ser menor que o uso de disco especificado por um relatório de cota devido à inclusão de blocos indiretos no relatório de cota. Por outro lado, se o arquivo tiver blocos vazios, o tamanho exibido pelo `ls` comando pode ser mais do que o uso do disco especificado pelo relatório de cota.

A saída do `ls` comando exibe apenas o tamanho de um arquivo e não inclui blocos indiretos usados pelo arquivo. Quaisquer blocos vazios do arquivo também são incluídos na saída do comando.

Exemplo da diferença entre o uso de espaço contabilizado pelo comando ls e um relatório de cota

O relatório de cota a seguir mostra um limite de 10 MB para uma qtree Q1:

```
                                     ----Disk----  ----Files-----   Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  vol1     q1          tree    user1   10MB  10MB        1       -   q1

...
```

Um arquivo presente na mesma qtree pode ter um tamanho que exceda o limite de cota quando visto de um cliente UNIX usando o `ls` comando, como mostrado no exemplo a seguir:

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

Como o comando df responde pelo tamanho do arquivo

A maneira como no `df` comando relata o uso do espaço depende de duas condições: Se as cotas estão ativadas ou desativadas para o volume que contém a qtree e se o uso da cota dentro da qtree é rastreado.

Quando as cotas estão ativadas para o volume que contém a utilização de qtree e cota dentro da qtree é rastreada, o uso de espaço relatado pelo `df` comando equivale ao valor especificado pelo relatório de cota.

Nessa situação, o uso de cota exclui blocos usados por diretórios, ACLs, diretórios de fluxo e metafiles.

Quando as cotas não estão habilitadas no volume ou quando a qtree não tem uma regra de cota configurada, o uso de espaço relatado inclui blocos usados por diretórios, ACLs, diretórios de fluxo e metafiles para todo o volume, incluindo outros qtrees dentro do volume. Nessa situação, o uso de espaço relatado pelo `df` comando é maior do que o valor esperado relatado quando as cotas são rastreadas.

Quando você executa o `df` comando a partir do ponto de montagem de uma qtree para a qual o uso de cota é rastreado, a saída do comando mostra o mesmo uso de espaço que o valor especificado pelo relatório de cota. Na maioria dos casos, quando a regra de cota de árvore tem um limite de disco rígido, o tamanho total relatado pelo `df` comando é igual ao limite de disco e o espaço disponível é igual à diferença entre o limite de disco de cota e o uso de cota.

No entanto, em alguns casos, o espaço disponível relatado pelo `df` comando pode ser igual ao espaço disponível no volume como um todo. Isso pode ocorrer quando não há limite de disco rígido configurado para a qtree. Começando com ONTAP 9.9,1, ele também pode ocorrer quando o espaço disponível no volume como um todo for menor do que o espaço restante da cota de árvore. Quando qualquer uma dessas condições ocorre, o tamanho total relatado pelo `df` comando é um número sintetizado igual à cota usada dentro da qtree mais o espaço disponível no FlexVol volume.

> Este tamanho total não é nem o limite do disco de qtree nem o tamanho configurado do volume. Ele também pode variar com base na atividade de gravação em outros qtrees ou na atividade de eficiência de storage em segundo plano.

Exemplo de uso de espaço contabilizado pelo `df` comando e um relatório de cota

O relatório de cota a seguir mostra um limite de disco de 1 GB para qtree alice, 2 GB para qtree bob e nenhum limite para a qtree project1:

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     alice     tree    1
                                   502.0MB    1GB       2       -   alice
vol2     bob       tree    2
                                    1003MB    2GB       2       -   bob
vol2     project1  tree    3
                                   200.8MB      -       2       -
project1
vol2               tree    *           0B      -       0       -   *
4 entries were displayed.
```

No exemplo a seguir, a saída `df` do comando no qtrees alice e bob relata o mesmo espaço usado que o relatório de cota, e o mesmo tamanho total (em termos de blocos 1M) que o limite de disco. Isso ocorre porque as regras de cota para qtrees alice e bob têm um limite de disco definido e o volume disponível (1211 MB) é maior que o espaço de cota de árvore restante para a qtree alice (523 MB) e a qtree bob (1045 MB).

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1024   502       523  50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2048  1004      1045  50% /mnt/vol2
```

No exemplo a seguir, a saída do `df` comando na qtree project1 relata o mesmo espaço usado que o relatório de cota, mas o tamanho total é sintetizado adicionando o espaço disponível no volume como um todo (1211 MB) ao uso de cota de qtree project1 (201 MB) para dar um total de 1412 MB. Isso ocorre porque a regra de cota para a qtree project1 não tem limite de disco.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412   201      1211  15% /mnt/vol2
```

O exemplo a seguir mostra como a saída do `df` comando no volume como um todo relata o mesmo espaço disponível que project1.

```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
```

Disparidade entre o comando du e o relatório de cota para uso de espaço

Quando você executa o `du` comando para verificar o uso do espaço em disco para uma qtree ou FlexVol volume montado em um cliente UNIX, o valor de uso pode ser maior do que o valor exibido por um relatório de cota para a qtree ou volume.

A saída do `du` comando contém o uso de espaço combinado de todos os arquivos através da árvore de diretórios começando no nível do diretório onde o comando é emitido. Como o valor de uso exibido pelo `du` comando também inclui os blocos de dados para diretórios, ele é maior do que o valor exibido por um relatório de cota.

Exemplo da diferença entre o uso de espaço contabilizado pelo comando du e um relatório de cota

O relatório de cota a seguir mostra um limite de 10MB para uma qtree Q1:

```
                                        ----Disk----  ----Files-----   Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  vol1     q1        tree    user1    10MB   10MB   1       -        q1

...
```

No exemplo a seguir, o uso do espaço em disco como saída do `du` comando mostra um valor mais alto que excede o limite de cota:

```
[user1@lin-sys1 q1]$ du -sh
**11M**     q1
```

Exemplos de configuração de cotas

Esses exemplos ajudam você a entender como configurar cotas e ler relatórios de cotas.

Sobre estes exemplos

Para ver os exemplos a seguir, suponha que você tenha um sistema de storage que inclua um SVM, `vs1`, com um volume, `vol1`.

1. Para iniciar a configuração de cotas, crie uma nova política de cotas para o SVM:

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

2. Como a política de cota é nova, você a atribui ao SVM:

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

Exemplo 1: Cota de usuário padrão

1. Você decide impor um limite rígido de 50MB para cada usuário no `vol1`:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtree ""
```

2. Para ativar a nova regra, inicialize cotas no volume:

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

3. Você vê o relatório de cota:

```
cluster1::>volume quota report
```

O relatório de quota resultante é semelhante ao seguinte relatório:

```
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     49MB   50MB      37       -   *
vol1               user    root        0B      -       1       -
```

A primeira linha mostra a cota de usuário padrão que você criou, incluindo o limite de disco. Como todas as cotas padrão, essa cota de usuário padrão não exibe informações sobre o uso do disco ou do arquivo. Para além da quota criada, aparecem duas outras quotas. Há uma cota para cada usuário que atualmente possui arquivos no `vol1`. Essas cotas adicionais são cotas de usuário que foram derivadas automaticamente da cota de usuário padrão. A quota de utilizador derivada para o utilizador `jsmith` tem o mesmo limite de disco de 50MB GB que a quota de utilizador predefinida. A cota de usuário derivada para o usuário raiz é uma cota de rastreamento (sem limites).

Se qualquer usuário no sistema (que não seja o usuário raiz) tentar executar uma ação que usaria mais de 50MB em `vol1` (por exemplo, gravar em um arquivo de um editor), a ação falhará.

Exemplo 2: Quota de utilizador explícita que substitui uma quota de utilizador predefinida

1. Se for necessário fornecer mais espaço em volume `vol1` ao usuário `jsmith`, digite o seguinte comando:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree ""
```

   Essa é uma cota de usuário explícita, porque o usuário está explicitamente listado como o destino da regra de cota.

   Essa é uma alteração para um limite de cota existente, porque altera o limite de disco da cota de usuário derivada para o usuário `jsmith` no volume. Portanto, você não precisa reinicializar cotas no volume para ativar a alteração.

2. Para redimensionar cotas:

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

As cotas permanecem em vigor enquanto você redimensiona, e o processo de redimensionamento é curto.

O relatório de quota resultante é semelhante ao seguinte relatório:

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     50MB   80MB      37       -   jsmith
vol1               user    root        0B      -       1       -
3 entries were displayed.
```

A segunda linha agora mostra um limite de disco de `80MB` e um especificador de cota `jsmith` de .

Portanto `jsmith`, pode usar até 80MBMB de espaço `vol1`, mesmo que todos os outros usuários ainda estejam limitados a 50MBMB.

Exemplo 3: Limites

Suponha que você deseja receber uma notificação quando os usuários atingem dentro de 5MB de seus limites de disco.

1. Para criar um limite de 45MB para todos os usuários e um limite de 75MB para `jsmith`, você altera as regras de cota existentes:

   ```
   cluster1::>volume quota policy rule modify -vserver vs1 -policy
   quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree ""
   -threshold 45MB
   cluster1::>volume quota policy rule modify -vserver vs1 -policy
   quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
   -threshold 75MB
   ```

   Como os tamanhos das regras existentes são alterados, você redimensiona cotas no volume para ativar as alterações. Você espera até que o processo de redimensionamento seja concluído.

2. Para ver o relatório de cota com limites, adicione o `-thresholds` parâmetro ao `volume quota report` comando:

```
cluster1::>volume quota report -thresholds
Vserver: vs1
                                     ----Disk----  ----Files-----
Volume   Tree      Type    ID        Used  Limit   Used    Limit  Quota
                                          (Thold)
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -  *
                                         (45MB)
vol1               user    jsmith     59MB   80MB      55       -  jsmith
                                         (75MB)
vol1               user    root        0B      -       1       -
                                         ( -)
3 entries were displayed.
```

Os limites aparecem entre parênteses na coluna limite do disco.

Exemplo 4: Cotas em qtrees

Suponha que você precise particionar algum espaço para dois projetos. Você pode criar dois qtrees, `proj1` nomeados e `proj2`, para acomodar esses projetos dentro `vol1`do .

Atualmente, os usuários podem usar tanto espaço em uma qtree quanto eles são alocados para todo o volume (desde que eles não excedessem o limite para o volume usando espaço na raiz ou em outra qtree). Além disso, cada um dos qtrees pode crescer para consumir todo o volume.

1. Se você quiser garantir que nenhuma qtree cresça além de 20GB, você pode criar cota de árvore padrão no volume:

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```

O tipo correto é *tree*, não qtree.

2. Como essa é uma nova cota, você não pode ativá-la redimensionando. Você reinicializa cotas no volume:

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```

Você deve garantir que você aguarde cerca de cinco minutos antes de reativar as cotas em cada volume afetado, pois tentar ativá-las quase imediatamente após a execução do `volume quota off` comando pode resultar em erros. Como alternativa, você pode executar os comandos para reinicializar as cotas de um volume do nó que contém o volume específico.

As cotas não são aplicadas durante o processo de reinicialização, o que leva mais tempo do que o processo de redimensionamento.

Quando você exibe um relatório de cota, ele tem várias linhas novas. Algumas linhas são para cotas de árvore e algumas linhas são para cotas de usuário derivadas.

As seguintes novas linhas são para as cotas de árvore:

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1              tree    *           0B   20GB       0       -   *
vol1     proj1    tree    1           0B   20GB       1       -   proj1
vol1     proj2    tree    2           0B   20GB       1       -   proj2
...
```

A cota de árvore padrão que você criou aparece na primeira nova linha, que tem um asterisco (*) na coluna ID. Em resposta à cota de árvore padrão em um volume, o ONTAP cria automaticamente cotas de árvore derivadas para cada qtree no volume. Estes são mostrados nas linhas onde `proj1` e `proj2` aparecem na `Tree` coluna.

As novas linhas a seguir são para cotas de usuários derivadas:

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1     proj1    user    *           0B   50MB       0       -
vol1     proj1    user    root        0B      -       1       -
vol1     proj2    user    *           0B   50MB       0       -
vol1     proj2    user    root        0B      -       1       -
...
```

As cotas de usuário padrão em um volume são herdadas automaticamente para todos os qtrees contidos nesse volume, se as cotas estiverem habilitadas para qtrees. Quando você adicionou a primeira cota de qtree, ativou cotas no qtrees. Portanto, cotas de usuário padrão derivadas foram criadas para cada qtree. Estes são mostrados nas linhas em que ID é asterisco (*).

Como o usuário root é o proprietário de um arquivo, quando as cotas de usuário padrão foram criadas para cada qtrees, cotas especiais de rastreamento também foram criadas para o usuário root em cada qtrees. Estes são mostrados nas linhas em que ID é root.

Exemplo 5: Cota de usuário em uma qtree

1. Você decide limitar os usuários a menos espaço `proj1` na qtree do que no volume como um todo. Você deseja evitar que eles usem mais de 10MB na `proj1` qtree. Portanto, você cria uma cota de usuário padrão para a qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
-qtree proj1
```

   Esta é uma alteração para uma cota existente, porque altera a cota de usuário padrão para a qtree proj1 que foi derivada da cota de usuário padrão no volume. Portanto, você ativa a alteração reredimensionando cotas. Quando o processo de redimensionamento estiver concluído, você poderá exibir o relatório de cota.

   A nova linha a seguir aparece no relatório de cota mostrando a nova cota de usuário explícita para a qtree:

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    *           0B   10MB       0       -   *
```

   No entanto, o usuário `jsmith` está sendo impedido de gravar mais dados na qtree proj1 porque a cota que você criou para substituir a cota de usuário padrão (para fornecer mais espaço) estava no volume. À medida que você adicionou uma cota de usuário padrão na `proj1` qtree, essa cota está sendo aplicada e limitando todo o espaço dos usuários nessa qtree, `jsmith` incluindo .

2. Para fornecer mais espaço ao usuário `jsmith`, você adiciona uma regra de cota de usuário explícita para a qtree com limite de disco 80MB para substituir a regra de cota de usuário padrão para a qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree proj1
```

   Como essa é uma cota explícita para a qual já existia uma cota padrão, você ativa a alteração reredimensionando cotas. Quando o processo de redimensionamento estiver concluído, você exibirá um relatório de cota.

A nova linha a seguir aparece no relatório de cota:

```
                                  ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
```

O relatório de quota final é semelhante ao seguinte relatório:

```
cluster1::>volume quota report
Vserver: vs1
                                  ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               tree    *           0B   20GB       0       -   *
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    70MB   80MB      65       -   jsmith
vol1     proj1     tree    1           0B   20GB       1       -   proj1
vol1     proj1     user    *           0B   10MB       0       -   *
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
vol1               user    root        0B      -       3       -
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
11 entries were displayed.
```

O usuário `jsmith` deve atender aos seguintes limites de cota para gravar em um arquivo no `proj1`:

1. A cota de árvore para a `proj1` qtree.
2. A cota de usuário na `proj1` qtree.
3. A quota de utilizador no volume.

Configure cotas em um SVM

É possível configurar cotas em uma nova SVM para gerenciar e monitorar a utilização de recursos.

Sobre esta tarefa

Em alto nível, há várias etapas envolvidas na configuração de cotas, incluindo:

1. Crie uma política de quota

2. Adicione as regras de cota à política
3. Atribua a política ao SVM
4. Inicialize as cotas em cada FlexVol volume no SVM

Passos

1. Digite o comando `vserver show -instance` para exibir o nome da política de cota padrão criada automaticamente quando o SVM foi criado.

   Se um nome não foi especificado quando o SVM foi criado, o nome será "padrão". Você pode usar o `vserver quota policy rename` comando para dar um nome à política padrão.

   > Você também pode criar uma nova política usando o `volume quota policy create` comando.

2. Use o `volume quota policy rule create` comando para criar *any* das seguintes regras de cota para cada volume na SVM:
   - Regras de cota padrão para todos os usuários
   - Regras de quota explícitas para utilizadores específicos
   - Regras de cota padrão para todos os grupos
   - Regras de quota explícitas para grupos específicos
   - Regras de cota padrão para todos os qtrees
   - Regras de cota explícitas para qtrees específicos
3. Use o `volume quota policy rule show` comando para verificar se as regras de cota estão configuradas corretamente.
4. Se você estiver trabalhando em uma nova política, use o `vserver modify` comando para atribuir a nova política ao SVM.
5. Use o `volume quota on` comando para inicializar as cotas em cada volume na SVM.

   Você pode monitorar o processo de inicialização das seguintes maneiras:

   - Ao utilizar o `volume quota on` comando, pode adicionar o `-foreground` parâmetro para executar a quota no trabalho em primeiro plano. (Por padrão, o trabalho é executado em segundo plano.)

     Quando o trabalho é executado em segundo plano, você pode monitorar seu progresso usando o `job show` comando.

   - Você pode usar o `volume quota show` comando para monitorar o status da inicialização da cota.
6. Use o `volume quota show -instance` comando para verificar se há erros de inicialização, como regras de cota que não foram inicializadas.
7. Use o `volume quota report` comando para exibir um relatório de cota para garantir que as cotas aplicadas correspondam às suas expetativa.

Modificar ou redimensionar limites de cota

Você pode alterar ou redimensionar as cotas em todos os volumes afetados, o que é mais rápido do que reinicializar cotas nesses volumes.

Sobre esta tarefa

Você tem uma máquina virtual de storage (SVM, anteriormente conhecida como SVM) com cotas aplicadas e deseja alterar os limites de tamanho das cotas existentes ou adicionar ou excluir cotas de destinos que já tenham cotas derivadas.

Passos

1. Use o `vserver show` comando com o `-instance` parâmetro para determinar o nome da política atualmente atribuída ao SVM.
2. Modifique as regras de cota executando qualquer uma das seguintes ações:
   - Use o `volume quota policy rule modify` comando para modificar os limites de disco ou arquivo das regras de cota existentes.
   - Use o `volume quota policy rule create` comando para criar regras de cota explícitas para alvos (usuários, grupos ou qtrees) que atualmente têm cotas derivadas.
   - Use o `volume quota policy rule delete` comando para excluir regras de cota explícitas para alvos (usuários, grupos ou qtrees) que também têm cotas padrão.
3. Use o `volume quota policy rule show` comando para verificar se as regras de cota estão configuradas corretamente.
4. Use o `volume quota resize` comando em cada volume em que você alterou cotas para ativar as alterações em cada volume.

   Você pode monitorar o processo de redimensionamento de uma das seguintes maneiras:

   - Ao usar o `volume quota resize` comando, você pode adicionar o `-foreground` parâmetro para executar o trabalho de redimensionamento em primeiro plano. (Por padrão, o trabalho é executado em segundo plano.)

     Quando o trabalho é executado em segundo plano, você pode monitorar seu progresso usando o `job show` comando.

   - Você pode usar o `volume quota show` comando para monitorar o status de redimensionamento.
5. Use o `volume quota show -instance` comando para verificar se há erros de redimensionamento, como regras de cota que não conseguiram ser redimensionadas.

   Em particular, verifique se há erros de "nova definição", que ocorrem quando você redimensiona cotas depois de adicionar uma cota explícita para um destino que ainda não tenha uma cota derivada.
6. Use o `volume quota report` comando para exibir um relatório de cota para que você possa garantir que as cotas aplicadas correspondam aos seus requisitos.

Reinicialize as cotas depois de fazer alterações extensas

Depois de fazer alterações extensas nas definições de quota existentes, tem de reinicializar as quotas em todos os volumes afetados. Um exemplo desse tipo de alteração é adicionar ou excluir cotas para alvos que não têm cotas impostas.

Sobre esta tarefa

Você tem uma máquina virtual de storage (SVM) com cotas aplicadas e deseja fazer alterações que exijam uma reinicialização total das cotas.

Passos

1. Use o `vserver show` comando com o `-instance` parâmetro para determinar o nome da política atualmente atribuída ao SVM.
2. Modifique as regras de cota executando qualquer uma das seguintes ações:

Se você quiser…	Então…
Crie novas regras de quota	Use o `volume quota policy rule create` comando
Modifique as definições das regras de quota existentes	Use o `volume quota policy rule modify` comando
Eliminar regras de quota existentes	Use o `volume quota policy rule delete` comando

3. Use o `volume quota policy rule show` comando para verificar se as regras de cota estão configuradas corretamente.
4. Reinicialize cotas em cada volume em que você alterou cotas desativando cotas e ativando cotas para esses volumes.
   a. Use o `volume quota off` comando em cada volume afetado para desativar cotas nesse volume.
   b. Use o `volume quota on` comando em cada volume afetado para ativar cotas nesse volume.

> Você deve garantir que você aguarde cerca de cinco minutos antes de reativar as cotas em cada volume afetado, pois tentar ativá-las quase imediatamente após a execução do `volume quota off` comando pode resultar em erros.
>
> Como alternativa, você pode executar os comandos para reinicializar as cotas de um volume do nó que contém o volume específico.

   Você pode monitorar o processo de inicialização de uma das seguintes maneiras:

   - Ao utilizar o `volume quota on` comando, pode adicionar o `-foreground` parâmetro para executar a quota no trabalho em primeiro plano. (Por padrão, o trabalho é executado em segundo plano.)

     Quando o trabalho é executado em segundo plano, você pode monitorar seu progresso usando o `job show` comando.

   - Você pode usar o `volume quota show` comando para monitorar o status da inicialização da cota.

5. Use o `volume quota show -instance` comando para verificar se há erros de inicialização, como regras de cota que não foram inicializadas.
6. Use o `volume quota report` comando para exibir um relatório de cota para garantir que as cotas aplicadas correspondam às suas expetativa.

Comandos para gerenciar regras de cota e políticas de cota

Os `volume quota policy rule` comandos permitem configurar regras de quota e os `volume quota policy` comandos e alguns `vserver` comandos permitem configurar políticas de quota. Dependendo do que você precisa fazer, use os seguintes comandos para gerenciar regras de cota e políticas de cota:

Você pode executar os seguintes comandos apenas no FlexVol volumes.

Comandos para gerenciar regras de cota

Se você quiser…	Use este comando…
Crie uma nova regra de cota	`volume quota policy rule create`
Excluir uma regra de cota existente	`volume quota policy rule delete`
Modificar uma regra de cota existente	`volume quota policy rule modify`
Exibir informações sobre regras de cota configuradas	`volume quota policy rule show`

Comandos para gerenciar políticas de cota

Se você quiser…	Use este comando…
Duplique uma política de quota e as regras de quota que contém	`volume quota policy copy`
Crie uma nova política de quota em branco	`volume quota policy create`
Excluir uma política de cota existente que não esteja atribuída atualmente a uma máquina virtual de storage (SVM)	`volume quota policy delete`
Renomeie uma política de cota	`volume quota policy rename`
Exibir informações sobre políticas de cota	`volume quota policy show`
Atribua uma política de cota a um SVM	`vserver modify -quota-policy` *`policy_name`*
Exiba o nome da política de cota atribuída a um SVM	`vserver show`

Consulte o "Referência do comando ONTAP" para cada comando para obter mais informações.

Comandos para ativar e modificar cotas

`volume quota` os comandos permitem alterar o estado das cotas e configurar o registro de mensagens das cotas. Dependendo do que você precisa fazer, você pode usar os seguintes comandos para ativar e modificar cotas:

Se você quiser…	Use este comando…
Ativar cotas (também chamado de *inicializando* elas)	`volume quota on`
Redimensionar cotas existentes	`volume quota resize`
Desativar cotas	`volume quota off`
Altere o Registro de mensagens de cotas, ative cotas, desative cotas ou redimensione cotas existentes	`volume quota modify`

Consulte a página de manual de cada comando para obter mais informações.

Use deduplicação, compressão de dados e compactação de dados para aumentar a eficiência de storage

Deduplicação, compressão de dados, compactação de dados e eficiência de storage

Você pode executar deduplicação, compressão e compactação de dados em conjunto ou de forma independente para obter a melhor economia de espaço em uma FlexVol volume. A deduplicação elimina blocos de dados duplicados. A compactação de dados compacta os blocos de dados para reduzir a quantidade de storage físico necessária. A compactação de dados armazena mais dados em menos espaço para aumentar a eficiência de storage.

> ⓘ A partir do ONTAP 9.2, todos os recursos de eficiência de storage in-line, como deduplicação e compactação in-line, são habilitados por padrão nos volumes AFF.

Habilitar a deduplicação em um volume

Você pode habilitar a deduplicação em um FlexVol volume para obter eficiência de storage. É possível habilitar a deduplicação pós-processo em todos os volumes e a deduplicação in-line em volumes que residem em agregados AFF ou Flash Pool.

Se você quiser habilitar a deduplicação in-line em outros tipos de volumes, consulte o artigo da base de dados de Conhecimento "Como habilitar a deduplicação in-line de volume em agregados não AFF (All Flash FAS)".

Antes de começar

Para um FlexVol volume, você precisa ter verificado se existe espaço livre suficiente para metadados de deduplicação em volumes e agregados. Os metadados de deduplicação exigem uma quantidade mínima de espaço livre no agregado. Esse valor é igual a 3% do total de dados físicos para todos os volumes de FlexVol desduplicados ou componentes de dados dentro do agregado. Cada FlexVol volume ou componente de dados

deve ter 4% do valor total de dados físicos de espaço livre, para um total de 7%.

A partir do ONTAP 9.2, a deduplicação in-line é habilitada por padrão em sistemas AFF.

Opções

- Use o `volume efficiency on` comando para habilitar a deduplicação pós-processo.

  O seguinte comando permite a deduplicação pós-processo no volume VolA:

  ```
  volume efficiency on -vserver vs1 -volume VolA
  ```

- Use o `volume efficiency on` comando seguido pelo `volume efficiency modify` comando com a `-inline-deduplication` opção definida como `true` para habilitar a deduplicação pós-processo e a deduplicação in-line.

  Os comandos a seguir habilitam a deduplicação pós-processo e a deduplicação in-line no volume VolA:

  ```
  volume efficiency on -vserver vs1 -volume VolA

  volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
  ```

- Use o `volume efficiency on` comando seguido pelo `volume efficiency modify` comando com a `-inline-deduplication` opção definida como `true` e a `-policy` opção definida como `inline-only` para habilitar somente a deduplicação in-line.

  Os comandos a seguir habilitam somente a deduplicação in-line no volume VolA:

  ```
  volume efficiency on -vserver vs1 -volume VolA

  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline
  -dedupe true
  ```

Depois de terminar

Verifique se a configuração foi alterada visualizando as configurações de eficiência de volume: `volume efficiency show -instance`

Desativar a deduplicação em um volume

Você pode desativar a deduplicação pós-processo e a deduplicação in-line de forma independente em um volume.

O que você vai precisar

Parar qualquer operação de eficiência de volume que esteja atualmente ativa no volume: `volume efficiency stop`

Sobre esta tarefa

Se tiver ativado a compressão de dados no volume, executar o `volume efficiency off` comando desativa a compressão de dados.

Opções

- Use o `volume efficiency off` comando para desativar a deduplicação pós-processo e a

deduplicação in-line.

O seguinte comando desativa a deduplicação pós-processo e a deduplicação in-line no volume VolA:

```
volume efficiency off -vserver vs1 -volume VolA
```

- Use o `volume efficiency modify` comando com a `-policy` opção definida como `inline only` para desativar a deduplicação pós-processo, mas a deduplicação in-line permanece habilitada.

  O comando a seguir desativa a deduplicação pós-processo, mas a deduplicação in-line permanece habilitada no volume VolA:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
  ```

- Use o `volume efficiency modify` comando com a `-inline-deduplication` opção definida como `false` para desativar somente a deduplicação in-line.

  O seguinte comando desativa apenas a deduplicação in-line no volume VolA:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
  ```

Deduplicação em segundo plano automática em nível de volume em sistemas AFF

A partir do ONTAP 9.3, você pode configurar a deduplicação em segundo plano em nível de volume para ser executada automaticamente usando uma política de AFF predefinida `auto`. Nenhuma configuração manual dos horários é necessária. A `auto` política executa deduplicação contínua em segundo plano.

A `auto` política é definida para todos os volumes recém-criados e para todos os volumes atualizados que não foram configurados manualmente para deduplicação em segundo plano. Você pode "altere a política" `default`ou qualquer outra política para desativar o recurso.

Se um volume se mover de um sistema que não seja AFF para um sistema AFF, a `auto` diretiva será ativada no nó de destino por padrão. Se um volume passar de um nó AFF para um nó não AFF, a `auto` política no nó de destino será substituída pela `inline-only` política por padrão.

No AFF, o sistema monitora todos os volumes com a `auto` política e desprioriza o volume que tem menos economia ou tem substituições frequentes. Os volumes despriorizados não participam mais da deduplicação automática em segundo plano. O registo de alterações em volumes despriorizados é desativado e os metadados no volume são truncados.

Os usuários podem promover o volume despriorizado para reparticipar de uma desduplicação automática em segundo plano usando o `volume efficiency promote` comando disponível no nível avançado de privilégio.

Gerenciar a deduplicação in-line em nível de agregado em sistemas AFF

A deduplicação em nível de agregado elimina blocos duplicados em volumes pertencentes ao mesmo agregado. A partir do ONTAP 9.2, você pode executar deduplicação em nível de agregado em sistemas AFF. O recurso é habilitado por padrão para todos os volumes recém-criados e todos os volumes atualizados com a deduplicação in-line de volume ativada.

Sobre esta tarefa

A operação de deduplicação elimina blocos duplicados antes que os dados sejam gravados no disco. Somente os volumes com `space guarantee` o conjunto para `none` podem participar da deduplicação in-line em nível de agregado. Esta é a configuração padrão em sistemas AFF.

> A deduplicação in-line de nível agregado às vezes é chamada de deduplicação in-line entre volumes.

Passo

1. Gerenciar a deduplicação in-line em nível de agregado em sistemas AFF:

Se você quiser…	Use este comando
Habilitar a deduplicação in-line em nível de agregado	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true`
Desativar a deduplicação in-line em nível de agregado	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false`
Exibir o status de deduplicação in-line em nível de agregado	`volume efficiency config -volume vol_name`

Exemplos

O comando a seguir exibe o status de deduplicação in-line em nível agregado:

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                    vs0
Volume:                                     choke0_wfit_8020_03_0
Schedule:                                   -
Policy:                                     choke_VE_policy
Compression:                                true
Inline Compression:                         true
Inline Dedupe:                              true
Data Compaction:                            true
Cross Volume Inline Deduplication:          false
```

Gerenciar a deduplicação em segundo plano em nível de agregado em sistemas AFF

A deduplicação em nível de agregado elimina blocos duplicados em volumes pertencentes ao mesmo agregado. A partir do ONTAP 9.3, você pode executar deduplicação em nível agregado em segundo plano em sistemas AFF. O recurso é habilitado por padrão para todos os volumes recém-criados e todos os volumes atualizados com deduplicação de fundo de volume ativada.

Sobre esta tarefa

A operação é acionada automaticamente quando uma porcentagem grande suficiente do log de mudança foi preenchida. Nenhuma programação ou política está associada à operação.

A partir do ONTAP 9.4, os usuários do AFF também podem executar o verificador de deduplicação em nível agregado para eliminar duplicatas de dados existentes entre volumes no agregado. Pode utilizar o `storage aggregate efficiency cross-volume-dedupe start` comando com a `-scan-old-data=true` opção para iniciar o scanner:

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

A verificação de deduplicação pode ser demorada. Você pode querer executar a operação em horas fora do pico.

A deduplicação em segundo plano em nível agregado às vezes é chamada de deduplicação em segundo plano entre volumes.

Passos

1. Gerenciar a deduplicação em segundo plano em nível agregado em sistemas AFF:

Se você quiser…	Use este comando
Habilitar a deduplicação em segundo plano em nível de agregado	`volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe true`
Desativar a deduplicação em segundo plano em nível agregado	`volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe false`
Exibir o status de deduplicação em segundo plano no nível agregado	`aggregate efficiency cross-volume-dedupe show`

Visão geral da eficiência de storage sensível à temperatura

O ONTAP fornece benefícios de eficiência de storage sensíveis à temperatura ao avaliar a frequência com que os dados do volume são acessados e mapear essa frequência para o nível de compressão aplicado a esses dados. Para dados inativos acessados com pouca frequência, blocos de dados maiores são compatados e, para dados ativos, acessados com frequência e substituídos com mais frequência, blocos de dados menores são compatados, tornando o processo mais eficiente.

A eficiência de storage sensível à temperatura (SSE) é introduzida no ONTAP 9.8 e é ativada automaticamente em volumes AFF recém-criados com provisionamento reduzido. Você pode ativar a eficiência de storage sensível à temperatura em volumes AFF existentes e em volumes DP não AFF provisionados de forma fina.

A eficiência de storage sensível à temperatura não é aplicada nas plataformas AFF A70, AFF A90 e AFF A1K. A compactação não se baseia em dados ativos ou inativos nessas plataformas. Portanto, a compactação começa sem esperar que os dados fiquem inativos.

Introdução dos modos "padrão" e "eficiente"

A partir do ONTAP 9.10,1, os modos de eficiência de storage no nível de volume *default* e *efficient* são introduzidos apenas para sistemas AFF. Os dois modos oferecem a opção entre compactação de arquivos (padrão), que é o modo padrão ao criar novos volumes AFF ou eficiência de storage sensível à temperatura (eficiente), que permite a eficiência de storage sensível à temperatura. Com o ONTAP 9.10,1, "a eficiência de storage sensível à temperatura deve ser definida explicitamente" para ativar a compressão adaptável automática. No entanto, outros recursos de eficiência de storage, como compactação de dados, cronograma de deduplicação automática, deduplicação in-line entre volumes e deduplicação em segundo plano entre volumes, são habilitados por padrão nas plataformas AFF para os modos padrão e eficiente.

Ambos os modos de eficiência de storage (padrão e eficiente) são compatíveis com agregados habilitados para FabricPool e com todos os tipos de política de disposição em camadas.

Eficiência de storage sensível à temperatura ativada nas plataformas C-Series

A eficiência de storage sensível à temperatura é habilitada por padrão nas plataformas AFF C-Series e ao migrar volumes de uma plataforma que não seja TSSE para uma plataforma C-Series habilitada para TSSE usando a movimentação de volume ou SnapMirror com as seguintes versões instaladas no destino:

- ONTAP 9.12.1P4 e posterior
- ONTAP 9.13,1 e posterior

Para obter mais informações, "Comportamento de eficiência de storage com movimentação de volume e operações de SnapMirror"consulte .

No caso dos volumes existentes, a eficiência de storage sensível à temperatura não é ativada automaticamente. No entanto, é possível "modificar o modo de eficiência de storage"alterar manualmente para o modo eficiente.

Depois de alterar o modo de eficiência de storage para eficiente, você não poderá alterá-lo novamente.

Eficiência de storage aprimorada com embalagem sequencial de blocos físicos contíguos

A partir do ONTAP 9.13,1, a eficiência de storage sensível à temperatura adiciona empacotamento sequencial de blocos físicos contíguos para aprimorar ainda mais a eficiência de storage. Os volumes que têm a eficiência de storage sensível à temperatura ativada automaticamente têm o empacotamento sequencial habilitado quando você atualiza os sistemas para o ONTAP 9.13,1. Depois que a embalagem sequencial estiver ativada, é "reembalar manualmente os dados existentes"necessário .

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1 e posterior, os volumes existentes recebem um modo de eficiência de storage com base no tipo de compactação atualmente habilitado nos volumes. Durante uma atualização, os volumes com compressão ativada recebem o modo padrão e os volumes com eficiência de storage sensível à temperatura ativada recebem o modo eficiente. Se a compactação não estiver ativada, o modo de eficiência de storage permanecerá em branco.

Comportamento de eficiência de storage com movimentação de volume e operações de SnapMirror

O comportamento da eficiência de storage pode ser afetado por outras operações de storage ativas ou iniciadas ao mesmo tempo. Você deve estar ciente do impacto dessas operações na eficiência de storage.

Há várias situações em que a eficiência de storage em um volume pode ser afetada por outras operações. Isso inclui quando você realiza uma movimentação de volume ou operação SnapMirror e o que acontece quando você executa uma quebra de SnapMirror e ativa manualmente a eficiência de storage sensível à temperatura (SSE) depende do tipo de eficiência no volume de origem.

A tabela a seguir descreve o comportamento de um volume de origem e de um volume de destino quando você executa uma dessas operações.

Eficiência do volume de origem	Comportamento padrão do volume de destino			Comportamento padrão depois de ativar manualmente o TSSE (após o SnapMirror Break)		
	Tipo de eficiência de armazenamento	**Novas gravações**	* Compressão de dados frios*	**Tipo de eficiência de armazenamento**	**Novas gravações**	* Compressão de dados frios*
Sem eficiência de storage (provavelmente FAS)	Compactação de arquivos	A compressão de ficheiros é tentada em linha em dados recentemente gravados	Sem compactação de dados inativos, os dados permanecem como eles estão	TSSE com algoritmo de varredura de dados frios como ZSTD	A compressão em linha 8K é tentada no formato TSSE	**Dados compatados**: N/A * dados descompactados*: Compressão 32K tentada após os dias de limite cumpridos e **dados recém-escritos**: Compressão 32K tentada após os dias de limite cumpridos
Sem eficiência de storage (provavelmente FAS)	Compactação de arquivos em plataformas da série C usando ONTAP 9.11.1P10 ou ONTAP 9.12.1P3	Nenhuma compressão de dados inativos habilitada por TSSE	**File Compressed data**: N/A.	TSSE com algoritmo de varredura de dados frios como ZSTD	Compressão in-line de 8K TB	**Dados compatados**: N/A * dados descompactados*: Compressão 32K tentada após os dias de limite cumpridos e **dados recém-escritos**: Compressão 32K tentada após os dias de limite cumpridos

Sem eficiência de storage (provavelmente FAS)	TSSE em plataformas da série C usando ONTAP 9.12.1P4 e posterior ou ONTAP 9.13,1 e posterior	A compressão em linha 8K é tentada no formato TSSE	**Dados compatados**: N/A * dados descompactados*: Compressão 32K tentada após os dias de limite cumpridos e **dados recém-escritos**: Compressão 32K tentada após os dias de limite cumpridos	TSSE com algoritmo de varredura de dados frios como ZSTD	A compressão em linha 8K é tentada no formato TSSE	**Dados compatados**: N/A * dados descompactados*: Compressão 32K tentada após os dias de limite cumpridos e **dados recém-escritos**: Compressão 32K tentada após os dias de limite cumpridos
Grupo de compressão de ficheiros	O mesmo que a fonte	A compressão de ficheiros é tentada em linha em dados recentemente gravados	Sem compactação de dados inativos, os dados permanecem como eles estão	TSSE com algoritmo de varredura de dados frios como ZSTD	A compressão em linha 8K é tentada no formato TSSE	**File Compressed data**: Not Compressed * Uncompressed data*: A compressão 32K é tentada após os dias de limite cumpridos e **dados recém-escritos**: A compressão 32K é tentada após os dias de limite cumpridos
Verificação de dados frios TSSE	TSSE usando o mesmo algoritmo de compressão que o volume de origem (LZOPro→LZOPro e ZSTD→ZSTD)	Tentativa de compressão em linha 8K no formato TSSE	Tentativa de compressão de 32K com LzoPro após os dias limite, a frieza baseada é atendida tanto nos dados existentes quanto nos dados recém-gravados.	O TSSE está ativado. Nota: O algoritmo de varredura de dados frios LZOPro pode ser alterado para ZSTD.	A compressão em linha 8K é tentada no formato TSSE	A compressão de 32K é tentada após os dias limite, a frieza é atendida tanto nos dados existentes quanto nos dados recém-gravados.

Definir o modo de eficiência de armazenamento durante a criação de volume

A partir do ONTAP 9.10,1, você pode definir o modo de eficiência de storage ao criar um novo volume AFF.

Sobre esta tarefa

Você pode controlar o modo de eficiência de storage em um novo volume AFF usando o parâmetro `-storage-efficiency-mode`. O volume pode ser configurado para usar o modo de eficiência ou o modo de desempenho padrão. Os dois modos oferecem a opção entre compactação de arquivos ou eficiência de storage sensível à temperatura. A compactação de arquivos é o modo padrão quando novos volumes do AFF são criados. A eficiência de storage sensível à temperatura permite a eficiência de storage sensível à temperatura. Observação o parâmetro `-storage-efficiency-mode` não é compatível com volumes que não sejam AFF ou volumes de proteção de dados.

Passos

Você pode executar esta tarefa usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

A partir do ONTAP 9.10,1, você pode usar o System Manager para aumentar a eficiência de storage com o recurso de eficiência de storage sensível à temperatura. A eficiência de storage baseada em desempenho é habilitada por padrão.

1. Clique em **armazenamento > volumes**.
2. Localize o volume no qual deseja ativar ou desativar a eficiência de armazenamento e clique em .
3. Clique em **Editar > volumes** e role até **eficiência de armazenamento**.
4. Selecione **Ativar maior eficiência de armazenamento**.

CLI

Crie um novo volume usando o modo eficiente

Para definir o modo de eficiência de armazenamento sensível à temperatura ao criar um novo volume, você pode usar o `-storage-efficiency-mode` parâmetro com o valor `efficient`.

1. Crie um novo volume com o modo de eficiência ativado:

   ```
   volume create -vserver <vserver name> -volume <volume name> -aggregate
   <aggregate name> -size <volume size> -storage-efficiency-mode efficient
   ```

   ```
   volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1
   -storage-efficiency-mode efficient -size 10g
   ```

Crie um novo volume usando o modo de desempenho

O modo de performance é definido por padrão quando você cria novos volumes AFF com eficiência de storage. Embora não seja necessário, você pode opcionalmente usar o `default` valor com o `-storage -efficiency-mode` parâmetro quando você cria um novo volume AFF.

1. Crie um novo volume utilizando o modo de eficiência de armazenamento de desempenho, "falha de memória":

   ```
   volume create -vserver <vserver name> -volume <volume name> -aggregate
   <aggregate name> -size <volume size> -storage-efficiency-mode default
   ```

   ```
   volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage
   -efficiency-mode default -size 10g
   ```

Alterar o limite de compressão de dados inativos de volume no ONTAP

Você pode alterar a frequência com que o ONTAP realiza uma verificação de dados inativos modificando o limite de frieza em volumes usando a eficiência de storage sensível à temperatura.

Antes de começar

Você precisa ser um administrador de cluster ou SVM e usar o nível de privilégio avançado da CLI do ONTAP.

Sobre esta tarefa

O limiar de frieza pode ser de 1 a 60 dias. O limite padrão é de 14 dias.

Passos

1. Defina o nível de privilégio:

```
set -privilege advanced
```

2. Modificar a compressão de dados inativos em um volume:

```
volume efficiency inactive-data-compression modify -vserver <vserver_name>
-volume <volume_name> -threshold-days <integer>
```

Saiba mais sobre "modificação da compressão de dados inativos" a referência de comando do ONTAP.

Verifique o modo de eficiência do volume

Você pode usar o `volume-efficiency-show` comando em um volume AFF para verificar se a eficiência está definida e para visualizar o modo de eficiência atual.

Passo

1. Verifique o modo de eficiência num volume:

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields
storage-efficiency-mode
```

Alterar o modo de eficiência de volume

A partir do ONTAP 9.10,1, os modos de eficiência de storage em nível de volume *default* e *efficient* são suportados apenas para sistemas AFF. Esses modos oferecem a opção entre compactação de arquivos (padrão), que é o modo padrão ao criar novos volumes AFF ou eficiência de storage sensível à temperatura (eficiente), que permite a eficiência de storage sensível à temperatura. Você pode usar o `volume efficiency modify` comando para alterar o modo de eficiência de storage de um volume AFF de `default` para `efficient`ou definir um modo de eficiência quando a eficiência de volume ainda não estiver definida.

Passos

1. Alterar o modo de eficiência de volume:

```
volume efficiency modify -vserver <vserver name> -volume <volume name>
-storage-efficiency-mode <default|efficient>
```

Visualize a economia do espaço físico do volume com ou sem a eficiência de storage sensível à temperatura

Dependendo da versão do ONTAP, você pode visualizar a economia de espaço físico em cada volume. Você pode fazer isso para avaliar a eficácia de seus processos administrativos ou como parte do Planejamento de capacidade.

Sobre esta tarefa

A partir do ONTAP 9.11,1, você pode usar o comando `volume show-footprint` para visualizar a economia de espaço físico em volumes com a eficiência de storage sensível à temperatura (TSSE) ativada. A partir do ONTAP 9.13,1, você pode usar o mesmo comando para visualizar a economia de espaço físico em volumes não habilitados com TSSE.

Passos

1. Veja a economia de espaço físico do volume:

```
volume show-footprint
```

Exemplo de saída com TSSE ativado

```
      Vserver : vs0
      Volume  : vol_tsse_75_per_compress

      Feature                                    Used       Used%
      --------------------------------        ----------    -----
      Volume Data Footprint                     10.15GB      13%
      Volume Guarantee                               0B       0%
      Flexible Volume Metadata                  64.25MB       0%
      Delayed Frees                             235.0MB       0%
      File Operation Metadata                       4KB       0%

      Total Footprint                           10.45GB      13%

      Footprint Data Reduction                   6.85GB       9%
           Auto Adaptive Compression             6.85GB       9%
      Effective Total Footprint                  3.59GB       5%
```

Exemplo de saída sem TSSE ativado

```
Vserver : vs0
Volume  : vol_file_cg_75_per_compress

Feature                                      Used       Used%
--------------------------------           ----------    -----
Volume Data Footprint                         5.19GB        7%
Volume Guarantee                                 0B        0%
Flexible Volume Metadata                     32.12MB        0%
Delayed Frees                                90.17MB        0%
File Operation Metadata                          4KB        0%

Total Footprint                               5.31GB        7%

Footprint Data Reduction                      1.05GB        1%
     Data Compaction                          1.05GB        1%
Effective Total Footprint                     4.26GB        5%
```

Informações relacionadas

- "Definir o modo de eficiência de armazenamento durante a criação de volume"

Ativar a compactação de dados em um volume

Você pode ativar a compactação de dados em um FlexVol volume para obter economia de espaço usando o `volume efficiency modify` comando. Você também pode atribuir um tipo de compactação ao volume, se não quiser o tipo de compactação padrão.

Antes de começar

Você deve ter habilitado a deduplicação no volume.

- A deduplicação só precisa ser ativada e não precisa ser executada no volume.
- O scanner de compactação deve ser usado para compactar os dados existentes nos volumes presentes nas plataformas AFF.

"Habilitando a deduplicação em um volume"

Sobre esta tarefa

- Em agregados HDD e agregados Flash Pool, você pode habilitar a compactação in-line e pós-processo ou apenas a compactação pós-processo em um volume.

  Se você está habilitando ambos, então você deve ativar a compressão pós-processo no volume antes de ativar a compressão inline.

- Nas plataformas AFF, somente a compactação in-line é suportada.

  Antes de ativar a compressão em linha, você deve ativar a compressão pós-processo no volume. No

entanto, como a compressão pós-processo não é suportada em plataformas AFF, nenhuma compressão pós-processo ocorre nesses volumes e uma mensagem EMS é gerada informando que a compressão pós-processo foi ignorada.

- A eficiência de armazenamento sensível à temperatura é introduzida no ONTAP 9.8. Com esse recurso, a eficiência de storage é aplicada de acordo com os dados ativos ou inativos. Para dados inativos, blocos de dados maiores são compatados e, para dados ativos, que são sobrescritos com mais frequência, blocos de dados menores são compatados, tornando o processo mais eficiente. A eficiência de storage sensível à temperatura é ativada automaticamente em volumes AFF com thin Provisioning recém-criados.
- O tipo de compressão é atribuído automaticamente com base na plataforma do agregado:

Plataforma/agregados	Tipo de compressão
AFF	Compressão adaptável
Agregados Flash Pool	Compressão adaptável
Agregados HDD	Compressão secundária

Opções

- Use o `volume efficiency modify` comando para habilitar a compactação de dados com o tipo de compactação padrão.

  O comando a seguir habilita a compactação pós-processo no volume VolA do SVM VS1:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true
  ```

  O comando a seguir habilita a compactação pós-processo e inline no volume VolA do SVM VS1:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true -inline
  -compression true
  ```

- Use o `volume efficiency modify` comando no nível de privilégio avançado para habilitar a compactação de dados com um tipo de compactação específico.

  a. Use o `set -privilege advanced` comando para alterar o nível de privilégio para avançado.

  b. Use o `volume efficiency modify` comando para atribuir um tipo de compactação a um volume.

     O comando a seguir habilita a compactação pós-processo e atribui o tipo de compactação adaptável ao volume VolA do SVM VS1:

     ```
     volume efficiency modify -vserver vs1 -volume VolA -compression true
     -compression-type adaptive
     ```

     O comando a seguir habilita a compactação pós-processo e inline e atribui o tipo de compactação adaptável ao volume VolA do SVM VS1:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true
  -compression-type adaptive -inline-compression true
  ```

  a. Use o `set -privilege admin` comando para alterar o nível de privilégio para admin.

Mova entre compressão secundária e compressão adaptável

Você pode alternar entre compactação secundária e compactação adaptável, dependendo da quantidade de leituras de dados. A compressão adaptável é preferida quando há um alto volume de leituras aleatórias no sistema e um desempenho mais alto é necessário. A compressão secundária é preferida quando os dados são gravados sequencialmente e são necessárias economias de compressão mais elevadas.

Sobre esta tarefa

O tipo de compressão padrão é selecionado com base em seus agregados e plataforma.

Passos

1. Desativar a eficiência no volume:

   ```
   volume efficiency off
   ```

   Por exemplo, o seguinte comando desativa a eficiência no volume vol1:

   ```
   volume efficiency off -vserver vs1 -volume vol1
   ```

2. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

3. Descomprimir os dados comprimidos:

   ```
   volume efficiency undo
   ```

   Por exemplo, o comando a seguir descompacta os dados compatados no volume vol1:

   ```
   volume efficiency undo -vserver vs1 -volume vol1 -compression true
   ```

   > Você deve verificar se tem espaço suficiente no volume para acomodar os dados descompactados.

4. Altere para o nível de privilégio admin:

   ```
   set -privilege admin
   ```

5. Verifique se o estado da operação está inativo:

   ```
   volume efficiency show
   ```

   Por exemplo, o comando a seguir exibe o status de uma operação de eficiência no volume vol1:

   ```
   volume efficiency show -vserver vs1 -volume vol1
   ```

6. Ative a eficiência para o volume:

   `volume efficiency on` Por exemplo, o seguinte comando permite a eficiência no volume vol1:

   ```
   volume efficiency on -vserver vs1 -volume vol1
   ```

7. Ative a compressão de dados e, em seguida, defina o tipo de compressão:

   `volume efficiency modify`

   Por exemplo, o comando a seguir habilita a compactação de dados e define o tipo de compactação como compressão secundária no volume vol1:

   ```
   volume efficiency modify -vserver vs1 -volume vol1 -compression true
   -compression-type secondary
   ```

   > Esta etapa só permite a compactação secundária no volume; os dados no volume não são compatados.
   >
   > - Para comprimir dados existentes em sistemas AFF, tem de executar o scanner de compressão em segundo plano.
   > - Para compactar dados existentes em agregados Flash Pool ou agregados de HDD, é necessário executar a compactação em segundo plano.

8. Opcional: Ativar a compressão em linha:

   `volume efficiency modify`

   Por exemplo, o comando a seguir habilita a compactação inline no volume vol1:

   `volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true`

Desative a compressão de dados em um volume

Você pode desativar a compressão de dados em um volume usando o `volume efficiency modify` comando.

Sobre esta tarefa

Se você quiser desativar a compressão pós-processo, primeiro você deve desativar a compressão inline no volume.

Passos

1. Parar qualquer operação de eficiência de volume que esteja atualmente ativa no volume:

   `volume efficiency stop`

2. Desativar compressão de dados:

   `volume efficiency modify`

   Os dados compatados existentes permanecerão compatados no volume. Apenas as novas gravações que entram no volume não são comprimidas.

Exemplos

O seguinte comando desativa a compressão em linha no volume VolA:

`volume efficiency modify -vserver vs1 -volume VolA -inline-compression false`

O seguinte comando desativa a compressão pós-processo e a compressão em linha no volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline
-compression false
```

Gerenciar a compactação de dados in-line em sistemas AFF

Você pode controlar a compactação de dados in-line em sistemas AFF no nível do volume usando o `volume efficiency modify` comando. A compactação de dados é habilitada por padrão para todos os volumes em sistemas AFF.

Antes de começar

A compactação de dados exige que a garantia de espaço de volume seja definida como `none`. Este é o padrão para sistemas AFF.

> A garantia de espaço padrão em volumes de proteção de dados que não são da AFF é definida como nenhum.

Passos

1. Para verificar a definição de garantia de espaço para o volume:

   ```
   volume show -vserver vserver_name -volume volume_name –fields space-guarantee
   ```

2. Para ativar a compactação de dados:

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction true
   ```

3. Para desativar a compactação de dados:

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction false
   ```

4. Para apresentar o estado da compactação de dados:

   ```
   volume efficiency show -instance
   ```

Exemplos

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data
-compaction false
```

Permitir a compactação de dados in-line em sistemas FAS

Você pode ativar a compactação de dados in-line em sistemas FAS com agregados Flash Pool (híbridos) ou agregados HDD no nível de volume ou agregado, usando o `volume efficiency` comando cluster shell. A compactação de dados é desativada por padrão para sistemas FAS.

Sobre esta tarefa

Se você ativar a compactação de dados no nível agregado, a compactação de dados será ativada em qualquer novo volume criado com uma garantia de espaço de volume `none` de no agregado. Habilitar a compactação de dados em um volume em um agregado de HDD usa recursos adicionais de CPU.

Passos

1. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

2. Verifique o estado de compactação de dados dos volumes e agregados para o nó desejado:

```
volume efficiency show -volume <volume_name>
```

3. Permitir a compactação de dados no volume:

```
volume efficiency modify -volume <volume_name> -data-compaction true
```

> Se a compactação de dados estiver definida como `false` para um agregado ou um volume, a compactação falhará. Ativar a compactação não compacta os dados existentes; apenas novas gravações no sistema são compactadas. O `volume efficiency start` comando contém mais informações sobre como compactar dados existentes (no ONTAP 9.1 e posterior). Para obter mais informações, consulte "Referência do comando ONTAP" .

4. Veja as estatísticas de compactação:

```
volume efficiency show -volume <volume_name>
```

Eficiência de storage in-line habilitada por padrão em sistemas AFF

Por padrão, os recursos de eficiência de storage são ativados em todos os volumes recém-criados em sistemas AFF. A partir do ONTAP 9.2, todos os recursos de eficiência de storage in-line são habilitados por padrão em todos os volumes existentes e recém-criados em todos os sistemas AFF.

Os recursos de eficiência de storage incluem deduplicação in-line, deduplicação in-line entre volumes e compressão in-line, e são habilitados por padrão em sistemas AFF, conforme mostrado na tabela.

> O comportamento da compactação de dados em volumes AFF permanece inalterado no ONTAP 9.2, já que ele já está habilitado por padrão.

Condições de volume	Recursos de eficiência de storage habilitados por padrão no ONTAP 9.2		
	Deduplicação in-line	Deduplicação in-line entre volumes	Compressão in-line

Condições de volume	Recursos de eficiência de storage habilitados por padrão no ONTAP 9.2		
Atualização de cluster para 9,2	Sim	Sim	Sim
Transição do modo 7 do ONTAP para o Clustered ONTAP	Sim	Sim	Sim
Movimentação de volume	Sim	Sim	Sim
Volumes com provisionamento espesso	Sim	Não	Sim
Volumes criptografados	Sim	Não	Sim

As exceções a seguir se aplicam a um ou mais recursos de eficiência de storage in-line:

- Somente os volumes de leitura-gravação podem ser compatíveis com a capacitação padrão de eficiência de storage in-line.
- Os volumes com economia de compactação são omitidos da ativação da compactação in-line.
- Os volumes que têm a deduplicação pós-processo ativada são omitidos da ativação da compressão inline.
- Nos volumes em que a eficiência do volume é desativada, o sistema substitui as configurações de política de eficiência de volume existentes e a define para ativar a política somente inline.

Visualização de eficiência de storage

Use o `storage aggregate show-efficiency` comando para exibir informações sobre a eficiência de storage de todos os agregados em seu sistema.

O `storage aggregate show-efficiency` comando tem três visualizações diferentes que podem ser invocadas passando opções de comando.

Vista predefinida

A exibição padrão exibe a proporção geral para cada um dos agregados.

```
cluster1::> storage aggregate show-efficiency
```

Vista detalhada

Chame a exibição detalhada com a `-details` opção de comando. Esta vista apresenta o seguinte:

- Relação de eficiência geral para cada um dos agregados.
- Taxa geral sem cópias Snapshot.
- Divisão de proporção para as seguintes tecnologias de eficiência: Deduplicação de volume, compressão de volume, cópias Snapshot, clones, compactação de dados e deduplicação in-line agregada.

```
cluster1::> storage aggregate show-efficiency -details
```

Vista avançada

A vista avançada é semelhante à vista detalhada e apresenta detalhes lógicos e físicos utilizados.

Tem de executar este comando no nível avançado de privilégios. Alterne para privilégios avançados usando o `set -privilege advanced` comando.

O prompt de comando muda para `cluster::*>`.

```
cluster1::> set -privilege advanced
```

Invoque a visualização avançada com a `-advanced` opção de comando.

```
cluster1::*> storage aggregate show-efficiency -advanced
```

Para exibir taxas para um único agregado, invoque o comando individualmente `-aggregate` *`aggregate_name`*. Este comando pode ser executado no nível de administrador, bem como no nível de privilégio avançado.

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

Crie uma política de eficiência de volume para executar operações de eficiência

Crie uma política de eficiência de volume

Você pode criar uma política de eficiência de volume para executar deduplicação ou compactação de dados, seguida de deduplicação em um volume por uma duração específica e especificar a programação da tarefa usando o `volume efficiency policy create` comando.

Antes de começar

Você deve ter criado um cronograma cron usando o `job schedule cron create` comando. Para obter mais informações sobre como gerenciar os cronogramas do cron, consulte "Referência de administração do sistema".

Sobre esta tarefa

Um administrador da SVM com funções predefinidas não pode gerenciar as políticas de deduplicação. No entanto, o administrador do cluster pode modificar o Privileges atribuído a um administrador SVM usando quaisquer funções personalizadas. Para obter mais informações sobre os recursos do administrador da SVM, "Autenticação de administrador e RBAC"consulte .

> É possível executar operações de deduplicação ou compactação de dados em um horário agendado, ou criando um cronograma com uma duração específica, ou especificando uma porcentagem de limite, que aguarda que os novos dados excedam o limite e acionando a operação de deduplicação ou compactação de dados. Este valor limite é a percentagem do número total de blocos utilizados no volume. Por exemplo, se você definir o valor de limite em um volume para 20% quando o número total de blocos usados no volume for de 50%, a deduplicação de dados ou a compactação de dados serão acionados automaticamente quando novos dados gravados no volume chegarem a 10% (20% dos blocos de 50% usados). Se necessário, você pode obter o número total de blocos usados a partir da `df` saída do comando.

Passos

1. Use o `volume efficiency policy create` comando para criar uma política de eficiência de volume.

Exemplos

O comando a seguir cria uma política de eficiência de volume chamada pol1 que aciona uma operação de eficiência diariamente:

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

O comando a seguir cria uma política de eficiência de volume chamada pol2 que aciona uma operação de eficiência quando a porcentagem de limite atinge 20%:

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start
-threshold-percent 20%
```

Atribua uma política de eficiência de volume a um volume

Você pode atribuir uma política de eficiência a um volume para executar operações de deduplicação ou compressão de dados usando o `volume efficiency modify` comando.

Antes de começar

Certifique-se de que você "crie a política de eficiência de volume" antes de atribuí-lo a um volume.

Sobre esta tarefa

Se uma política de eficiência for atribuída a um volume secundário do SnapVault, somente o atributo prioridade de eficiência de volume será considerado ao executar operações de eficiência de volume. As programações de tarefas são ignoradas e a operação de deduplicação é executada quando atualizações incrementais são feitas no volume secundário do SnapVault.

Passo

1. Use o `volume efficiency modify` comando para atribuir uma política a um volume.

Exemplo

O comando a seguir atribui a política de eficiência de volume nomeada `new_policy` para `VolA` volume :

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

Modificar uma política de eficiência de volume

Você pode modificar uma política de eficiência de volume para executar a deduplicação e a compactação de dados por uma duração diferente ou alterar a programação da tarefa usando o `volume efficiency policy modify` comando.

Passos

1. Use o `volume efficiency policy modify` comando para modificar uma política de eficiência de volume.

Exemplos

O comando a seguir modifica a política de eficiência de volume chamada policy1 para ser executada a cada hora:

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

O comando a seguir modifica uma política de eficiência de volume chamada pol2 para o limite de 30%:

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start
-threshold-percent 30%
```

Ver uma política de eficiência de volume

Você pode exibir a política de eficiência de volume, incluindo o nome, a programação, a duração e a descrição.

Sobre esta tarefa

O comando `volume efficiency policy show` é usado para exibir uma política de eficiência de volume. Quando você executa o comando no escopo do cluster, as políticas com escopo de cluster não são exibidas. No entanto, você pode exibir as políticas com escopo de cluster no contexto SVM.

Passos

1. Use o `volume efficiency policy show` comando para exibir informações sobre uma política de eficiência de volume.

   A saída depende dos parâmetros especificados. Para obter mais informações sobre a exibição de exibição detalhada e outros parâmetros, consulte a página de manual para este comando.

Exemplos

O comando a seguir exibe informações sobre as políticas criadas para o SVM VS1:
```
volume efficiency policy show -vserver vs1
```

O comando a seguir exibe as políticas para as quais a duração é definida como 10 horas:
```
volume efficiency policy show -duration 10
```

Desassociar uma política de eficiência de volume de um volume

Você pode desassociar uma política de eficiência de volume de um volume para interromper a execução de quaisquer operações de deduplicação e compressão de dados baseadas em cronograma no volume. Depois de desassociar uma política de eficiência de volume, você precisa acioná-la manualmente.

Passo

1. Use o `volume efficiency modify` comando para desassociar uma política de eficiência de volume de um volume.

Exemplo

O comando a seguir desassocia a política de eficiência de volume do VolA: `volume efficiency modify -vserver vs1 -volume VolA -policy -`

Excluir uma política de eficiência de volume

Você pode excluir uma política de eficiência de volume usando o `volume efficiency policy delete` comando.

O que você vai precisar

Você deve ter certeza de que a política que deseja excluir não está associada a nenhum volume.

Você não pode excluir a política de eficiência predefinida *inline-only* e *default*.

Passo

1. Use o `volume efficiency policy delete` comando para excluir uma política de eficiência de volume.

Exemplo

O comando a seguir exclui uma diretiva de eficiência de volume chamada policy1: `volume efficiency policy delete -vserver vs1 -policy policy1`

Gerencie operações de eficiência de volume manualmente

Visão geral manual das operações de eficiência de volume

Você pode gerenciar como as operações de eficiência são executadas em um volume executando as operações de eficiência manualmente.

Você também pode controlar como as operações de eficiência são executadas com base nas seguintes condições:

- Use checkpoints ou não
- Execute operações de eficiência em dados existentes ou apenas novos dados
- Pare as operações de eficiência, se necessário

Você pode usar o `volume efficiency show` comando com `schedule` o valor como para a `-fields` opção para exibir a programação atribuída aos volumes.

Execute uma operação de eficiência manualmente

Você pode executar operações de eficiência em um volume manualmente. Você pode fazer isso quando agendar operações de eficiência não for apropriado.

Antes de começar

Dependendo da operação de eficiência que você deseja executar manualmente, você precisa ativar a deduplicação ou a compactação de dados e a deduplicação em um volume.

Sobre esta tarefa

Esta operação é efetuada através do `volume efficiency start` comando. Quando a eficiência de storage sensível à temperatura é habilitada em um volume, a deduplicação é executada inicialmente, seguida da compactação de dados.

A deduplicação é um processo em segundo plano que consome recursos do sistema enquanto está em execução. Se os dados não mudarem com frequência em um volume, é melhor executar a deduplicação com menos frequência. Várias operações de deduplicação simultâneas executadas em um sistema de storage levam a um maior consumo de recursos do sistema.

Você pode executar um máximo de oito operações de deduplicação simultânea ou compressão de dados por nó. Se forem agendadas mais operações de eficiência, as operações serão enfileiradas.

A partir do ONTAP 9.13,1, se a eficiência de storage sensível à temperatura estiver habilitada em um volume, você poderá executar a eficiência de volume nos dados existentes para aproveitar a embalagem sequencial para aprimorar ainda mais a eficiência de storage.

Execute a eficiência manualmente

Passos

1. Inicie a operação de eficiência em um volume: `volume efficiency start`

Exemplo

O comando a seguir permite que você inicie manualmente apenas a deduplicação ou a deduplicação, seguida de compactação lógica e compactação de contentor no volume VolA

E

```
volume efficiency start -vserver vs1 -volume VolA
```

Reembalar dados existentes

Para aproveitar o empacotamento de dados sequenciais introduzido no ONTAP 9.13,1 em volumes com eficiência de storage sensível à temperatura ativada, é possível reembalar os dados existentes. Você deve estar no modo de privilégio avançado para usar este comando.

Passos

1. Defina o nível de privilégio: `set -privilege advanced`
2. Reembalar dados existentes: `volume efficiency inactive-data-compression start -vserver` *`vserver_name`* `-volume` *`volume_name`* `-scan-mode extended_recompression`

Exemplo

```
volume efficiency inactive-data-compression start -vserver vs1 -volume
vol1 -scan-mode extended_recompression
```

Informações relacionadas

- "Execute operações de eficiência manualmente nos dados existentes"

Pontos de verificação e operações de eficiência

Os pontos de verificação são usados internamente para Registrar o processo de execução de uma operação de eficiência. Quando uma operação de eficiência é interrompida por qualquer motivo (como parada do sistema, interrupção do sistema, reinicialização ou porque a última operação de eficiência falhou ou parou) e os dados do ponto de verificação existem, a operação de eficiência pode ser retomada a partir do último arquivo do ponto de verificação.

Um checkpoint é criado:

- em cada etapa ou subetapa da operação

- quando você executa o `sis stop` comando
- quando a duração expira

Retomar uma operação de eficiência parada

Se uma operação de eficiência for interrompida devido a uma parada do sistema, interrupção do sistema ou reinicialização, você poderá retomar a operação de eficiência a partir do mesmo ponto em que foi interrompida. Isso ajuda a economizar tempo e recursos, não sendo necessário reiniciar a operação desde o início.

Sobre esta tarefa

Se você ativou apenas a deduplicação no volume, a deduplicação é executada nos dados. Se você habilitou a deduplicação e a compactação de dados em um volume, a compactação de dados será executada primeiro, seguida pela deduplicação.

Você pode ver os detalhes do ponto de verificação de um volume usando o `volume efficiency show` comando.

Por padrão, as operações de eficiência são retomadas a partir de pontos de verificação. No entanto, se um ponto de verificação correspondente a uma operação de eficiência anterior (a fase em que o `volume efficiency start` comando -scan-old-data é executado) for superior a 24 horas, então a operação de eficiência não será retomada do ponto de verificação anterior automaticamente. Neste caso, a operação de eficiência começa desde o início. No entanto, se você souber que mudanças significativas não ocorreram no volume desde a última varredura, você pode forçar a continuação do ponto de verificação anterior usando a `-use-checkpoint` opção.

Passos

1. Use o `volume efficiency start` comando com a `-use-checkpoint` opção para retomar uma operação de eficiência.

   O seguinte comando permite retomar uma operação de eficiência em novos dados no volume VolA:

   ```
   volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
   ```

   O seguinte comando permite retomar uma operação de eficiência em dados existentes no volume VolA:

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use
   -checkpoint true
   ```

Execute uma operação de eficiência manualmente nos dados existentes

É possível executar as operações de eficiência manualmente nos dados que existem em volumes de eficiência de storage sensíveis a temperatura antes de permitir a deduplicação, compressão de dados ou compactação de dados. Você pode executar essas operações com versões do ONTAP anteriores ao ONTAP 9.8.

Sobre esta tarefa

Esta operação é efetuada através do `volume efficiency start` comando com o `-scan-old-data` parâmetro. A `-compression` opção não funciona com `-scan-old-data` volumes de eficiência de storage sensíveis à temperatura. A compactação de dados inativos é executada automaticamente em dados pré-existentes para volumes de eficiência de storage sensíveis à temperatura no ONTAP 9.8 e versões

posteriores.

Se você ativar apenas a deduplicação em um volume, a deduplicação será executada nos dados. Se você habilitar a deduplicação, a compressão e a compactação de dados em um volume, a compressão de dados será executada primeiro, seguida de deduplicação e compactação de dados.

Quando você executa compactação de dados em dados existentes, por padrão, a operação de compactação de dados ignora os blocos de dados compartilhados por deduplicação e os blocos de dados bloqueados por cópias Snapshot. Se você optar por executar a compactação de dados em blocos compartilhados, a otimização será desativada e as informações de impressão digital serão capturadas e usadas para compartilhamento novamente. Você pode alterar o comportamento padrão da compactação de dados ao compactar dados existentes.

É possível executar um máximo de oito operações de deduplicação, compressão de dados ou compactação de dados simultaneamente por nó. As operações restantes são enfileiradas.

> A compactação pós-processo não é executada em plataformas AFF. É gerada uma mensagem EMS para informá-lo de que esta operação foi ignorada.

Passos

1. Use o `volume efficiency start -scan-old-data` comando para executar manualmente a deduplicação, a compressão de dados ou a compactação de dados nos dados existentes.

   O comando a seguir permite executar essas operações manualmente nos dados existentes no volume VolA:

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-
   compression | -dedupe | -compaction ] true
   ```

Informações relacionadas

- "Execute operações de eficiência manualmente"

Gerencie operações de eficiência de volume usando programações

Execute uma operação de eficiência com base na quantidade de novos dados gravados

Você pode modificar o cronograma de operação de eficiência para executar a deduplicação ou a compactação de dados quando o número de novos blocos gravados no volume após a operação de eficiência anterior exceder uma porcentagem de limite especificada. Isto aplica-se se a operação de eficiência anterior foi realizada manualmente ou programada.

Sobre esta tarefa

Se a `schedule` opção estiver definida como `auto`, a operação de eficiência programada será executada quando a quantidade de novos dados exceder a porcentagem especificada. O valor de limite padrão é 20%. Esse valor limite é a porcentagem do número total de blocos já processados pela operação de eficiência.

Passos

1. Use o `volume efficiency modify` comando com a `auto@num` opção para modificar o valor percentual de limiar.

`num` é um número de dois dígitos para especificar a porcentagem.

Exemplo

O comando a seguir modifica o valor percentual de limiar para 30% para o volume VolA:

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

Informações relacionadas

- "Execute operações de eficiência usando o agendamento"

Execute uma operação de eficiência usando o agendamento

É possível modificar o agendamento de operações de deduplicação ou compressão de dados em um volume. As opções de configuração de uma política de programação e eficiência de volume são mutuamente exclusivas.

Sobre esta tarefa

Esta operação é efetuada através do `volume efficiency modify` comando.

Passos

1. Use o `volume efficiency modify` comando para modificar o agendamento de operações de deduplicação ou compressão de dados em um volume.

Exemplos

O comando a seguir modifica o agendamento de operações de eficiência para que o VolA seja executado às 11 horas, de segunda a sexta-feira:

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

Informações relacionadas

- "Execute operações de eficiência dependendo da quantidade de novos dados gravados"

Monitorar operações de eficiência de volume

Visualizar operações e status de eficiência

Você pode ver se a deduplicação ou a compactação de dados estão ativadas em um volume. Você também pode exibir o status, o estado, o tipo de compactação e o progresso das operações de eficiência em um volume.

Existem duas tarefas disponíveis. Ambos usam o comando `volume efficiency show`.

Ver o estado de eficiência

Passos

1. Ver o estado de uma operação de eficiência num volume: `volume efficiency show`

   O comando a seguir exibe o status de uma operação de eficiência no volume VolA que é atribuído ao tipo de compressão adaptável:

   ```
   volume efficiency show -instance -vserver vs1 -volume VolA
   ```

Se a operação de eficiência estiver ativada no volume VolA e a operação estiver inativa, você poderá ver o seguinte na saída do sistema:

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

  Vserver Name: vs1
   Volume Name: VolA
   Volume Path: /vol/VolA
         State: Enabled
        Status: Idle
      Progress: Idle for 00:03:20
```

Determine se os volumes contêm dados embalados sequencialmente

Você pode exibir uma lista de volumes que têm o empacotamento sequencial ativado, por exemplo, quando precisar reverter para uma versão do ONTAP anterior a 9.13.1. Você deve estar no modo de privilégio avançado para usar este comando.

Passos

1. Defina o nível de privilégio: `set -privilege advanced`
2. Listar volumes que têm o empacotamento sequencial ativado:

   `volume efficiency show -extended-auto-adaptive-compression true`

Visualize a economia de espaço de eficiência

Você pode ver a quantidade de economia de espaço obtida por meio da deduplicação e da compactação de dados em um volume. Você pode fazer isso para avaliar a eficácia de seus processos administrativos ou como parte do Planejamento de capacidade.

Sobre esta tarefa

Você precisa usar o comando `volume show` para exibir a economia de espaço em um volume. Observe que a economia de espaço nas cópias Snapshot não está incluída no cálculo da economia de espaço obtida em um volume. O uso de deduplicação não afeta as cotas de volume. As cotas são relatadas no nível lógico e permanecem inalteradas.

Passos

1. Use o `volume show` comando para ver a economia de espaço obtida em um volume usando deduplicação e compactação de dados.

Exemplo

O comando a seguir permite visualizar a economia de espaço obtida usando deduplicação e compactação de dados no volume VolA: `volume show -vserver vs1 -volume VolA`

```
cluster1::> volume show -vserver vs1 -volume VolA

                                Vserver Name: vs1
                                 Volume Name: VolA

...
            Space Saved by Storage Efficiency: 115812B
       Percentage Saved by Storage Efficiency: 97%
                  Space Saved by Deduplication: 13728B
            Percentage Saved by Deduplication: 81%
                Space Shared by Deduplication: 1028B
                   Space Saved by Compression: 102084B
        Percentage Space Saved by Compression: 97%

...
```

Ver estatísticas de eficiência de um FlexVol volume

Você pode ver os detalhes das operações de eficiência executadas em um FlexVol volume. Você pode fazer isso para avaliar a eficácia de seus processos administrativos ou como parte do Planejamento de capacidade.

Passos

1. Use o `volume efficiency stat` comando para visualizar as estatísticas de operações de eficiência em um FlexVol volume.

Exemplo

O comando a seguir permite visualizar as estatísticas das operações de eficiência no volume VolA: `volume efficiency stat -vserver vs1 -volume VolA`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

               Vserver Name: vs1
                Volume Name: VolA
                Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

Parar as operações de eficiência de volume

Você pode parar uma operação de deduplicação ou compressão pós-processo.

Sobre esta tarefa

Esta operação utiliza o comando `volume efficiency stop`. Este comando gera automaticamente um ponto de verificação.

Passos

1. Use o `volume efficiency stop` comando para parar uma operação de desduplicação ativa ou compressão pós-processo.

   Se você especificar `-all` a opção, as operações de eficiência ativas e enfileiradas serão abortadas.

Exemplos

O comando a seguir interrompe a operação de desduplicação ou compressão pós-processo que está atualmente ativa no volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA
```

O comando a seguir aborta as operações de deduplicação ativa e enfileirada ou de compressão pós-processo no volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

Informações adicionais sobre como remover a economia de espaço de um volume

Você pode optar por remover a economia de espaço obtida executando operações de eficiência em um volume. No entanto, você deve ter espaço suficiente para acomodar uma reversão.

Existem vários recursos relacionados disponíveis para ajudá-lo a Planejar e implementar a remoção da economia de espaço.

Informações relacionadas

- "Como ver economia de espaço com deduplicação, compressão e compactação no ONTAP 9"
- "Como anular a economia de eficiência de storage no ONTAP"

Rehospedar um volume de um SVM para outro SVM

Prepare-se para rehospedar um volume de um SVM para outro SVM

Uma operação de rehost de volume permite reatribuir um volume nas ou SAN de um SVM para outro SVM, sem exigir uma cópia SnapMirror. O procedimento exato de rehost depende do protocolo de acesso do cliente usado e do tipo de volume. O rehost de volume é uma operação que causa interrupções no acesso aos dados e no gerenciamento de volumes.

Antes de rehospedar um volume de um SVM para outro, você precisa estar em conformidade com as seguintes condições:

- O volume deve estar online.
- Protocolo SAN ou nas

  Para o protocolo nas, o volume deve ser desmontado.

- Se o volume estiver em um relacionamento SnapMirror, o relacionamento deve ser excluído ou quebrado antes do rehost do volume.

Você pode ressincronizar a relação SnapMirror após a operação de rehost de volume.

Rehospede um volume SMB

É possível rehospedar um volume que serve dados usando o protocolo SMB. Para permitir que os clientes continuem acessando os dados após a operação de rehospedagem, você deve configurar manualmente as políticas e as regras associadas.

Sobre esta tarefa

- A rehospedagem é uma operação disruptiva.
- Se a operação de rehospedagem falhar, talvez seja necessário reconfigurar as políticas de volume e as regras associadas no volume de origem.
- Se os domínios SVM de origem e SVM de destino forem diferentes, você poderá perder o acesso aos objetos no volume.
- A partir do ONTAP 9.8, é suportado o realojamento de um volume com encriptação de volume NetApp (NVE). Se você estiver usando um gerenciador de chaves integrado, os metadados criptografados serão modificados durante a operação de rehost. Os dados do utilizador não são alterados.

  Se você estiver usando o ONTAP 9.8 ou anterior, será necessário descriptografar o volume antes de executar a operação de rehost.

- Quando o SVM de origem tiver usuários e grupos locais, as permissões para os arquivos e diretórios (ACLs) definidos não serão mais efetivas após a operação de rehost de volume.

  O mesmo se aplica às ACLs de auditoria (SACLs)

- Após a operação de rehost, as seguintes políticas de volume, regras de política e configurações são perdidas do volume de origem e devem ser reconfiguradas manualmente no volume rehospedado:
  - Políticas de exportação de volume e qtree
  - Políticas de antivírus
  - Política de eficiência de volume
  - Políticas de qualidade do serviço (QoS)
  - Políticas do Snapshot
  - Regras de quota
  - política e regras de exportação de configuração de serviços de nomes e de switch ns
  - IDs de usuário e grupo

Antes de começar

- O volume deve estar online.
- As operações de gerenciamento de volumes, como movimentação de volume ou movimentação de LUN, não devem estar em execução.
- O acesso aos dados ao volume que está sendo rehospedado deve ser interrompido.
- A configuração do ns-switch e dos serviços de nome do SVM de destino deve ser configurada para dar suporte ao acesso aos dados do volume de rehospedagem.
- O SVM de origem e o SVM de destino devem ter o mesmo domínio do active Directory e do realmDNS.
- O ID de usuário e o ID de grupo do volume devem estar disponíveis no SVM de destino ou alterados no

volume de hospedagem.

> Se os usuários e grupos locais estiverem configurados e houver arquivos e diretórios nesse volume com permissões definidas para esses usuários ou grupos, essas permissões não serão mais efetivas.

Passos

1. Registre informações sobre os compartilhamentos CIFS para evitar a perda de informações sobre compartilhamentos CIFS caso a operação de rehost de volume falhe.
2. Desmontar o volume do volume pai:

   ```
   volume unmount
   ```

3. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

4. Rehospede o volume no SVM de destino:

   ```
   volume rehost -vserver source_svm -volume vol_name -destination-vserver
   destination_svm
   ```

5. Monte o volume sob o caminho de junção apropriado no SVM de destino:

   ```
   volume mount
   ```

6. Criar compartilhamentos CIFS para o volume rehospedado:

   ```
   vserver cifs share create
   ```

7. Se os domínios DNS diferirem entre a SVM de origem e a SVM de destino, crie novos usuários e grupos.
8. Atualize o cliente CIFS com os novos LIFs SVM de destino e o caminho de junção para o volume rehospedado.

Depois de terminar

Você deve reconfigurar manualmente as políticas e as regras associadas no volume rehospedado.

"Configuração SMB"

"Configuração multiprotocolo SMB e NFS"

Rehospedar um volume NFS

É possível rehospedar um volume que forneça dados usando o protocolo NFS. Para permitir que os clientes continuem acessando os dados após a operação de rehospedagem, você deve associar o volume à política de exportação do SVM, bem como configurar manualmente as políticas e as regras associadas.

Sobre esta tarefa

- A rehospedagem é uma operação disruptiva.

- Se a operação de rehospedagem falhar, talvez seja necessário reconfigurar as políticas de volume e as regras associadas no volume de origem.
- A partir do ONTAP 9.8, é suportado o realojamento de um volume com encriptação de volume NetApp (NVE). Se você estiver usando um gerenciador de chaves integrado, os metadados criptografados serão modificados durante a operação de rehost. Os dados do utilizador não são alterados.

  Se você estiver usando o ONTAP 9.8 ou anterior, será necessário descriptografar o volume antes de executar a operação de rehost.

- Após a operação de rehost, as seguintes políticas de volume, regras de política e configurações são perdidas do volume de origem e devem ser reconfiguradas manualmente no volume rehospedado:
  - Políticas de exportação de volume e qtree
  - Políticas de antivírus
  - Política de eficiência de volume
  - Políticas de qualidade do serviço (QoS)
  - Políticas do Snapshot
  - Regras de quota
  - política e regras de exportação de configuração de serviços de nomes e de switch ns
  - IDs de usuário e grupo

Antes de começar

- O volume deve estar online.
- As operações de gerenciamento de volumes, como movimentos de volume ou movimentos LUN, não devem estar em execução.
- O acesso aos dados ao volume que está sendo rehospedado deve ser interrompido.
- A configuração do ns-switch e dos serviços de nome do SVM de destino deve ser configurada para dar suporte ao acesso aos dados do volume de rehospedagem.
- O ID de usuário e o ID de grupo do volume devem estar disponíveis no SVM de destino ou alterados no volume de hospedagem.

Passos

1. Registre informações sobre as políticas de exportação de NFS para evitar a perda de informações sobre políticas NFS no caso de falha na operação de rehost de volume.
2. Desmontar o volume do volume pai:

   ```
   volume unmount
   ```

3. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

4. Rehospede o volume no SVM de destino:

   ```
   volume rehost -vserver source_svm -volume volume_name -destination-vserver
   destination_svm
   ```

   A política de exportação padrão do SVM de destino é aplicada ao volume rehospedado.

5. Crie a política de exportação:

   ```
   vserver export-policy create
   ```

6. Atualize a política de exportação do volume rehospedado para uma política de exportação definida pelo usuário:

   ```
   volume modify
   ```

7. Monte o volume sob o caminho de junção apropriado no SVM de destino:

   ```
   volume mount
   ```

8. Verifique se o serviço NFS está em execução no SVM de destino.
9. Retomar o acesso NFS ao volume rehospedado.
10. Atualize as credenciais do cliente NFS e as configurações de LIF para refletir os LIFs SVM de destino.

    Isso ocorre porque o caminho de acesso ao volume (LIFs e caminho de junção) sofreu alterações.

Depois de terminar

Você deve reconfigurar manualmente as políticas e as regras associadas no volume rehospedado. Consulte "Configuração NFS" para obter mais informações.

Rehospede um volume SAN

É possível rehospedar um volume de SAN que fornece dados por meio de LUNs mapeados. Depois de recriar o grupo de iniciadores (igrop) no SVM de destino, a operação de rehost de volume pode remapear automaticamente o volume no mesmo SVM.

Sobre esta tarefa

- A rehospedagem é uma operação disruptiva.
- Se a operação de rehospedagem falhar, talvez seja necessário reconfigurar as políticas de volume e as regras associadas no volume de origem.
- A partir do ONTAP 9.8, é suportado o realojamento de um volume com encriptação de volume NetApp (NVE). Se você estiver usando um gerenciador de chaves integrado, os metadados criptografados serão modificados durante a operação de rehost. Os dados do utilizador não são alterados.

  Se você estiver usando o ONTAP 9.8 ou anterior, será necessário descriptografar o volume antes de executar a operação de rehost.

- Após a operação de rehost, as seguintes políticas de volume, regras de política e configurações são perdidas do volume de origem e devem ser reconfiguradas manualmente no volume rehospedado:
  - Políticas de antivírus
  - Política de eficiência de volume
  - Políticas de qualidade do serviço (QoS)
  - Políticas do Snapshot
  - política e regras de exportação de configuração de serviços de nomes e de switch ns

- IDs de usuário e grupo

Antes de começar

- O volume deve estar online.
- As operações de gerenciamento de volumes, como movimentos de volume ou movimentos LUN, não devem estar em execução.
- Não deve haver e/S ativa nos volumes ou LUNs.
- Você deve ter verificado que o SVM de destino não tem um grupo com o mesmo nome, mas iniciadores diferentes.

  Se o grupo tiver o mesmo nome, você deve ter renomeado o grupo em um dos SVMs (origem ou destino).

- Tem de ter ativado a `force-unmap-luns` opção.
  - O valor padrão da `force-unmap-luns` opção é `false`.
  - Nenhuma mensagem de aviso ou confirmação é exibida quando você define a `force-unmap-luns` opção como `true`.

Passos

1. Gravar informações de mapeamento LUN no volume de destino:

   `lun mapping show volume` *`volume`* `vserver` *`source_svm`*

   Esta é uma etapa de precaução para evitar a perda de informações sobre o mapeamento LUN caso o rehost de volume falhe.

2. Excluir grupos associados ao volume alvo.
3. Rehospede o volume de destino para o SVM de destino:

   `volume rehost -vserver` *`source_svm`* `-volume` *`volume_name`* `-destination-vserver` *`destination_svm`*

4. Mapear LUNs no volume alvo para os grupos apropriados:
   - O rehost de volume preserva LUNs no volume de destino, no entanto, os LUNs permanecem não mapeados.
   - Use o conjunto de portas SVM de destino durante o mapeamento de LUNs.
   - Se a `auto-remap-luns` opção estiver definida como `true`, os LUNs serão mapeados automaticamente após o novo host.

Rehospede um volume em uma relação do SnapMirror

Você pode rehospedar um volume definido como parte de uma relação do SnapMirror. Há vários problemas que você precisa considerar antes de rehospedar o relacionamento.

Sobre esta tarefa

- A rehospedagem é uma operação disruptiva.
- Se a operação de rehospedagem falhar, talvez seja necessário reconfigurar as políticas de volume e as regras associadas no volume de origem.

- Após a operação de rehost, as seguintes políticas de volume, regras de política e configurações são perdidas do volume de origem e devem ser reconfiguradas manualmente no volume rehospedado:
  - Políticas de exportação de volume e qtree
  - Políticas de antivírus
  - Política de eficiência de volume
  - Políticas de qualidade do serviço (QoS)
  - Políticas do Snapshot
  - Regras de quota
  - política e regras de exportação de configuração de serviços de nomes e de switch ns
  - IDs de usuário e grupo

Antes de começar

- O volume deve estar online.
- As operações de gerenciamento de volumes, como movimentos de volume ou movimentos LUN, não devem estar em execução.
- O acesso aos dados ao volume que está sendo rehospedado deve ser interrompido.
- A configuração do ns-switch e dos serviços de nome do SVM de destino deve ser configurada para dar suporte ao acesso aos dados do volume de rehospedagem.
- O ID de usuário e o ID de grupo do volume devem estar disponíveis no SVM de destino ou alterados no volume de hospedagem.

Passos

1. Registre o tipo de relacionamento SnapMirror:

   `snapmirror show`

   Esta é uma etapa de precaução para evitar a perda de informações sobre o tipo de relacionamento SnapMirror caso o rehost de volume falhe.

2. A partir do cluster de destino, elimine a relação SnapMirror:

   `snapmirror delete`

   Você não deve quebrar a relação do SnapMirror; caso contrário, a capacidade de proteção de dados do volume de destino é perdida e a relação não pode ser restabelecida após a operação de rehospedagem.

3. A partir do cluster de origem, remova as informações de relação do SnapMirror:

   `snapmirror release -relationship-info-only true`

   Definir o `-relationship-info-only` parâmetro para `true` remover as informações de relação de origem sem excluir os snapshots.

4. Se o volume estiver montado, desmonte-o:

   `volume unmount -vserver <source_svm> -volume <vol_name>`

5. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

6. Rehospede o volume no SVM de destino:

```
volume rehost -vserver <source_svm> -volume <vol_name> -destination-vserver
<destination_svm>
```

7. Se a relação de peering SVM não estiver presente, crie o relacionamento de pares SVM entre a SVM de origem e o SVM de destino:

```
vserver peer create
```

8. Crie a relação SnapMirror entre o volume de origem e o volume de destino:

```
snapmirror create
```

É necessário executar o `snapmirror create` comando a partir do SVM que hospeda o volume DP. O volume rehospedado pode ser a origem ou o destino da relação SnapMirror.

9. Ressincronizar a relação SnapMirror.

Recursos não compatíveis com um rehost de volume

Existem vários recursos do ONTAP que não suportam o volume Rehost. Você deve estar ciente desses recursos antes de tentar uma operação de rehost.

Os recursos a seguir não são compatíveis com um rehost de volume:

- SVM DR
- Configurações do MetroCluster

> Clonar um volume como um volume FlexClone em um SVM diferente também não é compatível com configurações do MetroCluster.

- Volumes SnapLock
- Volumes de criptografia de volume NetApp (NVE) (em versões do ONTAP anteriores a 9,8)

  Nas versões do ONTAP anteriores a 9,8, você deve descriptografar o volume antes de rehospedá-lo. As chaves de criptografia de volumes dependem das chaves do SVM. Se um volume for movido para outro SVM e a configuração de chave multitenant estiver habilitada no SVM de origem ou destino, o volume e as chaves SVM não corresponderão.

  A partir do ONTAP 9.8, você pode rehospedar um volume com NVE.

- Volumes FlexGroup
- Clonar volumes

Combinações recomendadas de volume e arquivo ou configuração LUN

Visão geral das combinações recomendadas de volume e arquivo ou configuração LUN

Existem combinações específicas de configurações de FlexVol volume e arquivo ou LUN que você pode usar, dependendo dos requisitos de aplicação e administração. Entender os benefícios e os custos dessas combinações pode ajudar você a determinar a configuração certa para o seu ambiente.

As seguintes combinações de configuração de volume e LUN são recomendadas:

- Arquivos ou LUNs com espaço reservado com provisionamento de volume espesso
- LUNs ou arquivos não reservados ao espaço com provisionamento de thin volumes
- Arquivos ou LUNs com espaço reservado com provisionamento de volume semi-espesso

Você pode usar o thin Provisioning SCSI em seus LUNs em conjunto com qualquer uma dessas combinações de configuração.

Arquivos ou LUNs com espaço reservado com provisionamento de volume espesso

Benefícios:

- Todas as operações de gravação dentro de arquivos reservados ao espaço são garantidas; elas não falharão devido a espaço insuficiente.
- Não há restrições quanto à eficiência de storage e às tecnologias de proteção de dados no volume.

Custos e limitações:

- Espaço suficiente deve ser separado do agregado na frente para suportar o volume provisionado thickly.
- O espaço igual a duas vezes o tamanho do LUN é alocado do volume no momento da criação do LUN.

LUNs ou arquivos não reservados ao espaço com provisionamento de thin volumes

Benefícios:

- Não há restrições quanto à eficiência de storage e às tecnologias de proteção de dados no volume.
- O espaço é alocado apenas como é usado.

Custos e restrições:

- As operações de gravação não são garantidas; elas podem falhar se o volume ficar sem espaço livre.
- Você deve gerenciar o espaço livre no agregado de forma eficaz para evitar que o agregado fique sem espaço livre.

Arquivos ou LUNs com espaço reservado com provisionamento de volume semi-espesso

Benefícios:

Há menos espaço reservado antes do que para o provisionamento de volume espesso, e ainda é fornecida uma garantia de gravação melhor esforço.

Custos e restrições:

- Operações de gravação podem falhar com essa opção.

Você pode mitigar esse risco equilibrando adequadamente o espaço livre no volume em relação à volatilidade dos dados.

- Não é possível confiar na retenção de objetos de proteção de dados, como cópias Snapshot, arquivos FlexClone e LUNs.
- Você não pode usar os recursos de eficiência de storage de compartilhamento de bloco do ONTAP que não podem ser excluídos automaticamente, incluindo deduplicação, compactação e descarregamento de cópias/ODX.

Determine o volume e a configuração de LUN corretos para as suas necessidades

Responder a algumas perguntas básicas sobre o seu ambiente pode ajudá-lo a determinar a melhor configuração de FlexVol volume e LUN para o seu ambiente.

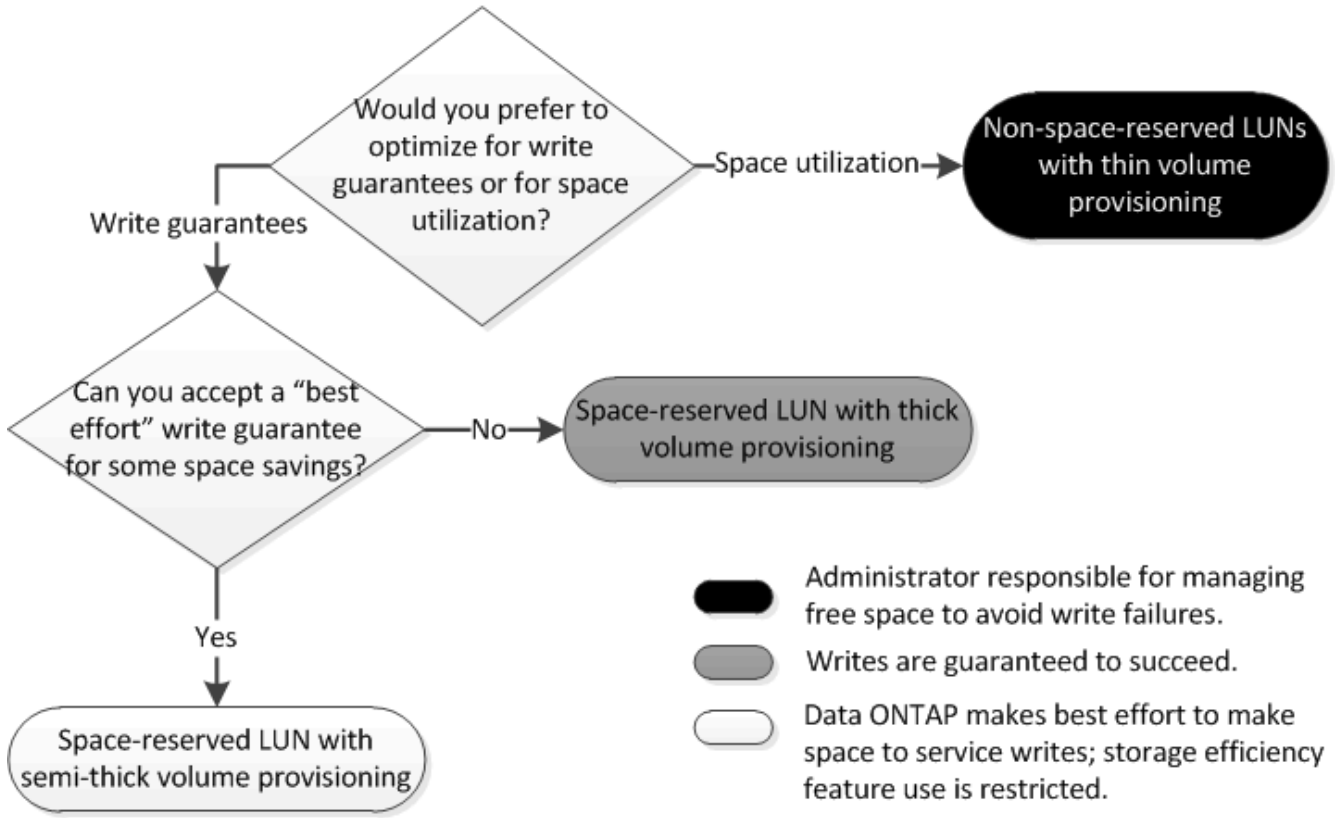
Sobre esta tarefa

Você pode otimizar as configurações de LUN e volume para a máxima utilização do storage ou para a segurança das garantias de gravação. Com base nos requisitos de utilização do storage e na capacidade de monitorar e reabastecer o espaço livre rapidamente, é necessário determinar os volumes de FlexVol volume e LUN apropriados para sua instalação.

Não é necessário um volume separado para cada LUN.

Passo

1. Use a seguinte árvore de decisão para determinar a melhor combinação de volume e configuração LUN para o seu ambiente:



Definições de configuração para ficheiros reservados ao espaço ou LUNs com volumes provisionados de espessura

Existem várias combinações de configuração de configurações de FlexVol volume e arquivo ou configurações LUN que você pode usar. Essa combinação com base em volumes com provisionamento excessivo permite usar tecnologias de eficiência de storage e não exige que você monitore ativamente seu espaço livre porque espaço suficiente é alocado inicialmente.

As configurações a seguir são necessárias para configurar um arquivo ou LUN com espaço reservado em um volume usando provisionamento espesso:

Definição do volume	Valor
Garantia	Volume
Reserva fracionária	100
Reserva do Snapshot	Qualquer
snapshot Autodelete	Opcional
Crescimento automático	Opcional; se ativado, o espaço livre agregado deve ser monitorado ativamente.

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Ativado

Informações relacionadas

- "Visão geral das combinações recomendadas de volume e arquivo ou configuração LUN"

Configurações para arquivos não reservados ao espaço ou LUNs com volumes provisionados com thin

Essa combinação de configuração de FlexVol volume e arquivo ou LUN exige que a menor quantidade de storage seja alocada antes, mas requer gerenciamento ativo de espaço livre para evitar erros devido à falta de espaço.

As seguintes configurações são necessárias para configurar um LUN ou arquivos não reservados ao espaço em um volume provisionado com thin:

Definição do volume	Valor
Garantia	Nenhum
Reserva fracionária	0

Definição do volume	Valor
Reserva do Snapshot	Qualquer
snapshot Autodelete	Opcional
Crescimento automático	Opcional

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Desativado

Considerações adicionais

Quando o volume ou agregado ficar sem espaço, as operações de gravação no arquivo ou LUN podem falhar.

Se você não quiser monitorar ativamente o espaço livre tanto para o volume quanto para o agregado, ative o crescimento automático para o volume e defina o tamanho máximo para o volume como o tamanho do agregado. Nessa configuração, você deve monitorar ativamente o espaço livre agregado, mas não precisa monitorar o espaço livre no volume.

Configurações para arquivos reservados ao espaço ou LUNs com provisionamento de volume semi-espesso

Existem várias combinações de configuração de configurações de FlexVol volume e arquivo ou configurações LUN que você pode usar. Essa combinação com base no provisionamento de volume semi-espesso requer menos storage para ser alocado antes do que a combinação totalmente provisionada. Mas coloca restrições às tecnologias de eficiência que você pode usar para o volume. As substituições são cumpridas com o melhor esforço para essa combinação de configuração.

As configurações a seguir são necessárias para configurar um LUN com espaço reservado em um volume usando provisionamento semi-espesso:

Definição do volume	Valor
Garantia	Volume
Reserva fracionária	0
Reserva do Snapshot	0
snapshot Autodelete	On, com um nível de compromisso de destruir, uma lista de destruir que inclui todos os objetos, o gatilho definido para volume e todos os LUNs e arquivos FlexClone FlexClone ativados para exclusão automática.

Definição do volume	Valor
Crescimento automático	Opcional; se ativado, o espaço livre agregado deve ser monitorado ativamente.

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Ativado

Restrições tecnológicas

Você não pode usar as seguintes tecnologias de eficiência de storage de volume para essa combinação de configuração:

- Compactação
- Deduplicação
- Descarregar cópias ODX e FlexClone
- LUNs e arquivos FlexClone do FlexClone não marcados para exclusão automática (clones ativos)
- Subficheiros FlexClone
- Descarregar ODX/Copy

Considerações adicionais

Os seguintes fatos devem ser considerados ao empregar esta combinação de configuração:

- Quando o volume compatível com o LUN é executado com pouco espaço, os dados de proteção (LUNs e arquivos FlexClone, cópias Snapshot) são destruídos.
- As operações de gravação podem ter tempo limite e falhar quando o volume ficar sem espaço livre.

A compactação é ativada por padrão para plataformas AFF. Você deve desativar explicitamente a compactação para qualquer volume para o qual deseja usar o provisionamento semi-espesso em uma plataforma AFF.

Informações relacionadas

- "Visão geral das combinações recomendadas de volume e arquivo ou configuração LUN"

Precauções e considerações para alterar a capacidade do arquivo ou diretório

O número máximo de ficheiros permitido para volumes FlexVol

Os volumes FlexVol têm um número máximo de arquivos que podem conter. Você pode alterar esse máximo, mas antes de fazer isso, você deve entender como essa alteração afeta o volume.

Se seus dados exigirem um grande número de arquivos ou diretórios muito grandes, você poderá expandir a capacidade do arquivo ou diretório ONTAP. No entanto, você deve entender as limitações e advertências para fazê-lo antes de prosseguir.

O número de arquivos que um volume pode conter é determinado por quantos inodes ele tem. Um *inode* é

uma estrutura de dados que contém informações sobre arquivos. Os volumes têm inodes privados e públicos. Inodes públicos são usados para arquivos que são visíveis para o usuário; inodes privados são usados para arquivos que são usados internamente pelo ONTAP. Você pode alterar apenas o número máximo de inodes públicos para um volume. Você não pode afetar o número de inodes privados.

O ONTAP define automaticamente o número máximo de inodes públicos para um volume recém-criado com base no tamanho do volume: 1 inodes por 32 KB de tamanho do volume. Quando o tamanho de um volume é aumentado, seja diretamente por um administrador ou automaticamente por ONTAP através do recurso de dimensionamento automático, o ONTAP também aumenta (se necessário) o número máximo de inodes públicos, portanto, há pelo menos 1 inode por 32 KB de tamanho do volume, até que o volume atinja aproximadamente 680 GB de tamanho.

Nas versões do ONTAP anteriores a 9.13.1, aumentar o volume superior a 680 GB de tamanho não resulta automaticamente em mais inodes, porque o ONTAP não cria automaticamente mais de 22.369.621 inodes. Se você precisar de mais arquivos do que o número padrão para qualquer volume de tamanho, você pode usar o comando volume Modify para aumentar o número máximo de inodes para o volume.

A partir de ONTAP 9.13,1, o número máximo de inodes continua a crescer, portanto, há um inode por 32 KB de espaço de volume, mesmo que o volume seja maior que 680 GB. Este crescimento continua até que o volume atinja o máximo de inodes de 2.147.483.632.

Você também pode diminuir o número máximo de inodes públicos. Diminuir o número de inodes públicos *não* altera a quantidade de espaço alocado para inodes, mas reduz a quantidade máxima de espaço que o arquivo de inodes público pode consumir. Depois que o espaço foi alocado para inodes, ele nunca é retornado ao volume. Portanto, diminuir o número máximo de inodes abaixo do número de inodes atualmente alocados não retorna o espaço utilizado pelos inodes alocados.

Mais informações

- Determine o uso de arquivos e inode para um volume

Tamanho máximo do diretório para volumes FlexVol

Você pode aumentar o tamanho máximo padrão do diretório para um FlexVol volume específico usando a `-maxdir-size` opção `volume modify` do comando, mas isso pode afetar o desempenho do sistema. Consulte o artigo da base de dados de Conhecimento "O que é maxdirsize?".

Para saber mais sobre os tamanhos máximos de diretórios dependentes do modelo para volumes FlexVol, visite o "NetApp Hardware Universe".

Restrições em volumes de raiz de nós e agregados de raiz

Você deve estar ciente das restrições que regem o volume raiz e o agregado raiz de um nó.

> O volume raiz de um nó contém diretórios e arquivos especiais para o nó. O volume raiz está contido no agregado raiz.

O volume raiz de um nó é um FlexVol volume instalado na fábrica ou pelo software de configuração. Ele é reservado para arquivos de sistema, arquivos de log e arquivos principais. O nome do diretório é `/mroot`, que é acessível somente através do systemshell pelo suporte técnico. O tamanho mínimo para o volume raiz de um nó depende do modelo da plataforma.

- As seguintes regras regem o volume raiz do nó:
  - A menos que o suporte técnico o instrua a fazê-lo, não modifique a configuração ou o conteúdo do volume raiz.
  - Não armazene dados do usuário no volume raiz.

    Armazenar dados de usuário no volume raiz aumenta o tempo de giveback de storage entre nós em um par de HA.

  - Você pode mover o volume raiz para outro agregado.

    "Realocação de volumes raiz para novos agregados"

- O agregado raiz é dedicado apenas ao volume raiz do nó.

  O ONTAP impede que você crie outros volumes no agregado raiz.

"NetApp Hardware Universe"

Realocar um volume raiz para novos agregados

O procedimento de substituição de raiz migra o agregado de raiz atual para outro conjunto de discos sem interrupção. Pode ser necessário executar isso como parte de um processo de substituição de disco ou manutenção preventiva.

Sobre esta tarefa

Você pode alterar o local do volume raiz para um novo agregado nos seguintes cenários:

- Quando os agregados de raiz não estão no disco que preferir
- Quando pretender reorganizar os discos ligados ao nó
- Quando estiver a efetuar uma substituição de prateleira das prateleiras de disco EOS

Passos

1. Realocar o agregado raiz:

   ```
   system node migrate-root -node node_name -disklist disk_list -raid-type
   raid_type
   ```

   - **-node**

     Especifica o nó que possui o agregado raiz que você deseja migrar.

   - **-disklist**

     Especifica a lista de discos nos quais o novo agregado raiz será criado. Todos os discos precisam ser sobressalentes e de propriedade do mesmo nó. O número mínimo de discos necessário depende do tipo RAID.

   - **-raid-type**

     Especifica o tipo RAID do agregado raiz. O valor padrão é `raid-dp`. Este é o único tipo suportado no modo avançado.

2. Monitorize o progresso do trabalho:

```
job show -id jobid -instance
```

Resultados

Se todas as pré-verificações forem bem-sucedidas, o comando iniciará uma tarefa de substituição de volume raiz e será encerrado.

Recursos compatíveis com arquivos FlexClone e LUNs FlexClone

Recursos compatíveis com arquivos FlexClone e LUNs FlexClone

O FlexClone Files e o FlexClone LUNs funcionam com diferentes recursos do ONTAP, como deduplicação, cópias Snapshot, cotas e SnapMirror de volume.

Os seguintes recursos são compatíveis com arquivos FlexClone e LUNs FlexClone:

- Deduplicação
- Cópias Snapshot
- Listas de controle de acesso
- Quotas
- Volumes FlexClone
- NDMP
- Volume SnapMirror
- O `volume move` comando
- Reserva de espaço
- Configuração HA

Deduplicação com arquivos FlexClone e FlexClone LUNs

Você pode usar com eficiência o espaço de storage físico dos blocos de dados criando um arquivo FlexClone ou LUN FlexClone do arquivo pai e LUN pai em um volume habilitado para deduplicação.

O mecanismo de compartilhamento de blocos usado pelos arquivos FlexClone e LUNs também é usado pela deduplicação. Você pode maximizar a economia de espaço em um FlexVol volume habilitando a deduplicação no volume e clonando o volume habilitado para deduplicação.

Ao executar o `sis undo` comando em um volume habilitado para deduplicação, você não pode criar arquivos FlexClone e LUNs FlexClone dos arquivos pai e LUNs pai residentes nesse volume.

Como as cópias Snapshot funcionam com arquivos FlexClone e FlexClone LUNs

Há uma sinergia entre as cópias Snapshot e os arquivos FlexClone e os LUNs FlexClone. Se você trabalha com essas tecnologias, você deve estar ciente do que é possível, bem como das restrições relevantes.

Criação de arquivos FlexClone e LUNs

Você pode criar um arquivo FlexClone ou FlexClone LUN a partir de uma cópia Snapshot existente. A cópia é baseada nos arquivos pai e LUNs pai contidos em um FlexVol volume.

Excluindo uma cópia Snapshot

Não é possível excluir manualmente uma cópia Snapshot da qual arquivos FlexClone ou LUNs FlexClone estejam sendo criados no momento. A cópia Snapshot permanece bloqueada até que o processo de compartilhamento de bloco em segundo plano seja concluído. Se você tentar excluir uma cópia Snapshot bloqueada, o sistema exibirá uma mensagem solicitando que você tente novamente a operação após algum tempo. Neste caso, você precisa continuar tentando novamente a operação de exclusão. Você poderá excluir a cópia Snapshot depois que o compartilhamento de bloco for concluído.

Herança de listas de controle de acesso por arquivos FlexClone e LUNs FlexClone

Os arquivos FlexClone e LUNs FlexClone herdam as listas de controle de acesso de seus arquivos pai e LUNs.

Se os arquivos pai contiverem fluxos do Windows NT, os arquivos FlexClone também herdarão as informações de fluxo. No entanto, os arquivos pai que contêm mais de seis fluxos não podem ser clonados.

Como as cotas funcionam com arquivos FlexClone e LUNs FlexClone

Você deve estar familiarizado com como as cotas funcionam com arquivos FlexClone e LUNs FlexClone antes de usá-los.

Os limites de cota são aplicados no tamanho lógico total dos arquivos FlexClone ou LUNs FlexClone. As operações de clonagem não falham no compartilhamento de blocos, mesmo que isso faça com que as cotas sejam excedidas.

Quando você cria um arquivo FlexClone ou FlexClone LUN, as cotas não reconhecem nenhuma economia de espaço. Por exemplo, se você criar um arquivo FlexClone de um arquivo pai de 10 GB, você estará usando apenas 10 GB de espaço físico, mas a utilização da cota será registrada como 20 GB (10 GB para o pai e 10 GB para o arquivo FlexClone).

Se a criação de um arquivo FlexClone ou LUN resultar na ultrapassagem da cota de grupo ou usuário, a operação de clone será bem-sucedida desde que o FlexVol volume tenha espaço suficiente para manter os metadados para o clone. No entanto, a cota para esse usuário ou grupo está sobrsubscrita.

Volumes do FlexClone e arquivos FlexClone associados e LUNs do FlexClone

Você pode criar um volume FlexClone de um FlexVol volume que tenha um arquivo FlexClone e um LUN FlexClone e seu arquivo pai ou LUN nele.

Os arquivos FlexClone ou LUNs FlexClone e seus arquivos pai ou LUNs presentes no volume FlexClone continuam compartilhando blocos da mesma maneira que fazem no FlexVol volume pai. Na verdade, todas as entidades FlexClone e seus pais compartilham os mesmos blocos de dados físicos subjacentes, minimizando o uso de espaço físico em disco.

Se o volume FlexClone for dividido do volume pai, os arquivos FlexClone ou LUNs FlexClone e seus arquivos pai ou LUNs pararão de compartilhar os blocos no clone do volume FlexClone. Depois disso, eles existem como arquivos independentes ou LUNs. Isso significa que o clone do volume usa mais espaço do que antes da operação de divisão.

Como o NDMP funciona com arquivos FlexClone e LUNs FlexClone

O NDMP funciona no nível lógico com arquivos FlexClone e LUNs FlexClone. Todos os arquivos FlexClone ou LUNs são copiados como arquivos separados ou LUNs.

Quando você usa serviços NDMP para fazer backup de uma qtree ou de um FlexVol volume que contenha arquivos FlexClone ou LUNs FlexClone, o compartilhamento de blocos entre entidades pai e clone não é preservado e o backup de entidades clone é feito na fita como arquivos separados ou LUNs. A economia de espaço é perdida. Portanto, a fita na qual você está fazendo backup deve ter espaço suficiente para armazenar a quantidade expandida de dados. Ao restaurar, todos os arquivos FlexClone e LUNs FlexClone são restaurados como arquivos físicos e LUNs separados. Você pode habilitar a deduplicação no volume para restaurar os benefícios de compartilhamento de bloco.

> Quando arquivos FlexClone e LUNs FlexClone estão sendo criados a partir de uma cópia Snapshot existente de um FlexVol volume, você não pode fazer backup do volume para fita até que o processo de compartilhamento de bloco, que acontece em segundo plano, esteja concluído. Se você usar o NDMP no volume quando o processo de compartilhamento de blocos estiver em andamento, o sistema exibirá uma mensagem solicitando que você repita a operação após algum tempo. Em tal situação, você deve continuar tentando novamente a operação de backup de fita para que ela seja bem-sucedida após a conclusão do compartilhamento de bloco.

Como o volume SnapMirror funciona com arquivos FlexClone e LUNs FlexClone

O uso do volume SnapMirror com FlexClone Files e FlexClone LUNs ajuda a manter a economia de espaço porque as entidades clonadas são replicadas apenas uma vez.

Se um FlexVol volume for uma fonte de volume SnapMirror e contiver arquivos FlexClone ou LUNs FlexClone, o volume SnapMirror transferirá apenas o bloco físico compartilhado e uma pequena quantidade de metadados para o destino do volume SnapMirror. O destino armazena apenas uma cópia do bloco físico, e esse bloco é compartilhado entre as entidades pai e clonadas. Portanto, o volume de destino é uma cópia exata do volume de origem e todos os arquivos clones ou LUNs no volume de destino compartilham o mesmo bloco físico.

Como a reserva de espaço funciona com arquivos FlexClone e LUNs FlexClone

Ao usar arquivos FlexClone e LUNs FlexClone, você deve entender como o atributo reserva de espaço funciona.

Por padrão, os arquivos FlexClone e LUNs herdam o atributo de reserva de espaço do arquivo pai e do LUN pai, respetivamente. No entanto, você pode criar arquivos FlexClone e LUNs FlexClone com reserva de espaço desativada se o FlexVol volume não tiver espaço. Isso é possível mesmo se o atributo no respetivo pai estiver habilitado.

Observe que se o FlexVol volume não contiver espaço suficiente para criar um arquivo FlexClone ou LUN FlexClone com a mesma reserva de espaço que a do pai, a operação de clonagem falhará.

Como funciona uma configuração de HA com arquivos FlexClone e FlexClone LUNs

As operações de arquivos FlexClone e FlexClone LUN são compatíveis em uma configuração de HA.

Em um par de HA, você não pode criar arquivos FlexClone ou LUNs FlexClone no parceiro enquanto a operação de takeover ou giveback estiver em andamento. Todas as operações pendentes de compartilhamento de blocos no parceiro são retomadas após a conclusão da operação de aquisição ou giveback.

Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup

Um volume FlexGroup é um contêiner nas escalável que fornece alto desempenho junto com distribuição automática de carga. Os volumes FlexGroup fornecem uma capacidade enorme (em petabytes), que excede consideravelmente os limites do FlexVol volume, sem adicionar nenhuma sobrecarga no gerenciamento.

Os tópicos nesta seção mostram como gerenciar volumes do FlexGroup com o Gerenciador de sistemas no ONTAP 9.7 e versões posteriores. Se você estiver usando o gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), veja este tópico:

- "Criar volumes FlexGroup"

A partir do ONTAP 9.9,1, as relações de fanout do SnapMirror de dois ou mais volumes FlexGroup são suportadas, com um máximo de oito pernas de fanout. O System Manager não é compatível com relacionamentos de volume FlexGroup em cascata do SnapMirror.

O ONTAP seleciona automaticamente os níveis locais necessários para criar o volume FlexGroup.

A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.

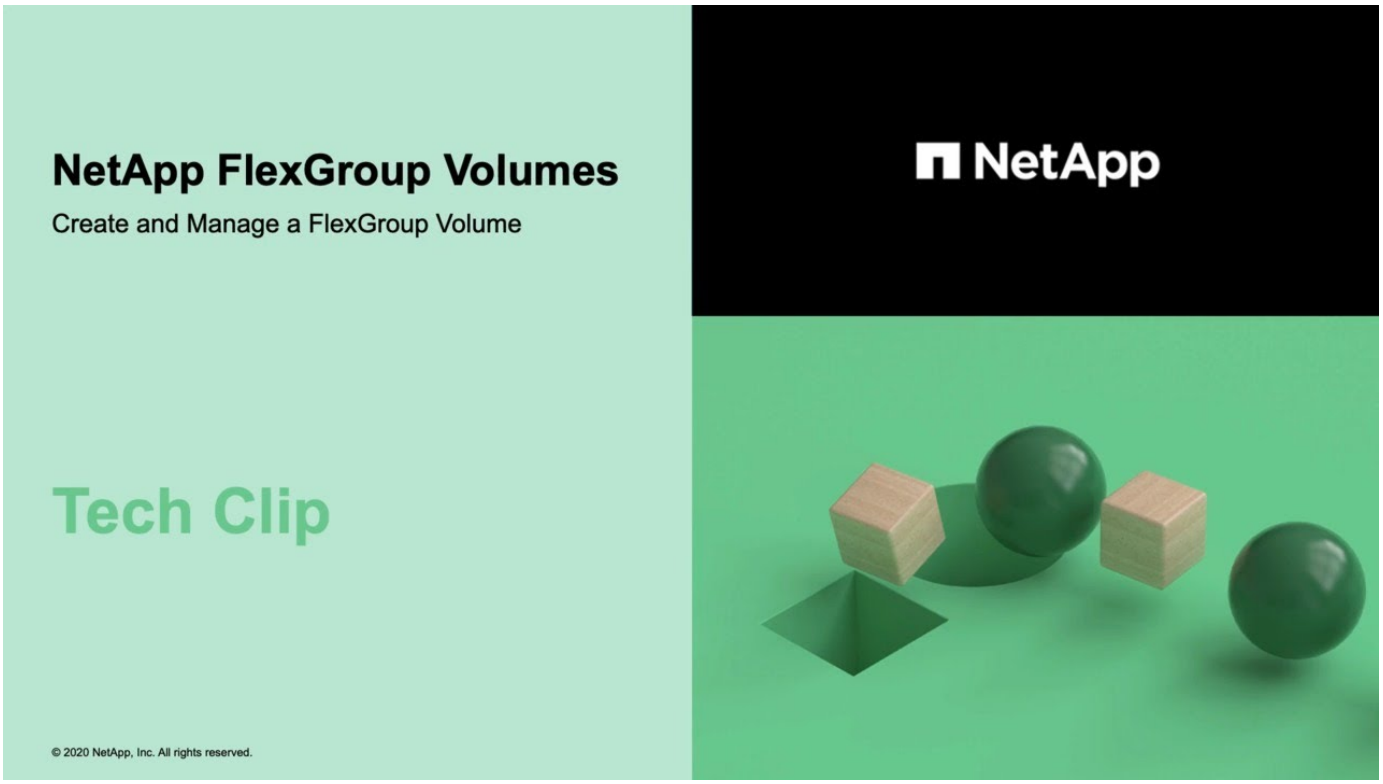
Passos

1. Clique em **armazenamento > volumes**.
2. Clique em **Add**.
3. Clique em **mais Opções** e selecione **distribuir dados de volume pelo cluster**.

> Se você estiver executando o ONTAP 9.8 ou posterior e quiser desativar o QoS ou escolher uma política de QoS personalizada, clique em **mais opções** e, em **armazenamento e otimização**, selecione **nível de serviço de desempenho**.

Vídeos

Criar e gerenciar um volume FlexGroup



FlexGroup volumes - Faça mais com menos

Gerenciamento de volumes do FlexGroup com a CLI

Visão geral do gerenciamento de volumes do FlexGroup com a CLI

Você pode configurar, gerenciar e proteger o FlexGroup volumes para escalabilidade e performance. Um volume FlexGroup é um volume com escalabilidade horizontal que oferece alto desempenho e distribuição automática de carga.

Você pode configurar volumes FlexGroup se as seguintes opções forem verdadeiras:

- Você está executando o ONTAP 9.1 ou posterior.
- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você tem o administrador de clusters Privileges, e não o Privileges do administrador da SVM.

> A partir do ONTAP 9.5, FlexGroups substituem Infinite volumes, que não são suportados no ONTAP 9.5 ou versões posteriores.

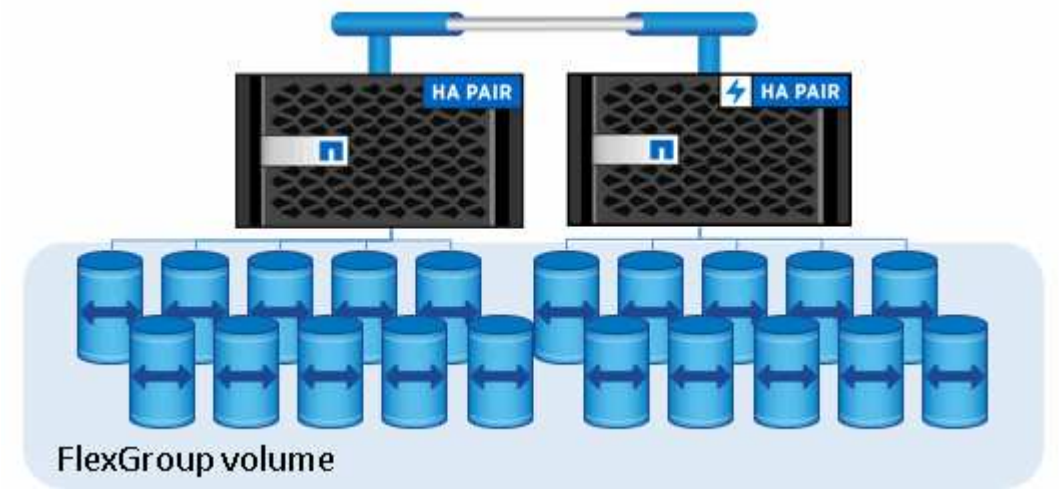
Consulte "Configurações com suporte e sem suporte para volumes FlexGroup" para obter mais informações.

Informações relacionadas

Informações conceituais sobre o FlexVol volumes são aplicáveis ao FlexGroup volumes. Informações sobre o FlexVol volumes e a tecnologia ONTAP estão disponíveis na Biblioteca de Referência do ONTAP e em relatórios técnicos (TRs).

O que é um volume FlexGroup

Um volume FlexGroup é um contêiner nas com escalabilidade horizontal que oferece alto desempenho, além de distribuição automática de carga e escalabilidade. Um volume FlexGroup contém vários volumes de membros (constituintes) que compartilham o tráfego de forma automática e transparente. *Volumes de membros* são os volumes FlexVol subjacentes que compõem um volume FlexGroup.



O FlexGroup volumes oferece os seguintes benefícios:

- Alta escalabilidade

  Vários volumes FlexGroup podem ser provisionados em um cluster, desde que o número de volumes membros não exceda os limites de nó ou cluster.

A partir do ONTAP 9.12.1P2, a capacidade máxima para um único volume FlexGroup é de 60PB TB, com 400 bilhões de arquivos em um cluster de 10 nós quando "o suporte de grande volume está ativado". Sem suporte a grandes volumes, a capacidade máxima para um único volume FlexGroup é de 20PB TB.

> Embora a capacidade máxima de um único volume de FlexGroup seja de 60PB TB (200 volumes de membros x 300TB de 60PB TB), o melhor desempenho é alcançado quando a capacidade utilizada dos volumes de membros permanece abaixo de 80% (200 volumes de membros x 240TB de 48PB TB).

- Alto desempenho

  O FlexGroup volumes pode utilizar os recursos do cluster para atender workloads com taxa de transferência alta e baixa latência.

- Gerenciamento simplificado

  Um volume FlexGroup é um contêiner de namespace único que pode ser gerenciado de maneira semelhante ao do FlexVol volumes.

Configurações com suporte e sem suporte para volumes FlexGroup

Você deve estar ciente dos recursos do ONTAP compatíveis e não compatíveis com o FlexGroup volumes no ONTAP 9.

Recursos suportados começando com ONTAP 9.16,1

- Balanceamento de capacidade avançado

Recursos suportados começando com ONTAP 9.15,1

- Aprimoramentos de provisionamento automático

Recursos suportados começando com ONTAP 9.14,1

- Marcação de cópias snapshot: Suporte para criar, modificar e excluir etiquetas de cópias Snapshot (rótulos e comentários do SnapMirror) para cópias Snapshot em volumes FlexGroup usando o `volume snapshot` comando.

Recursos suportados começando com ONTAP 9.13,1

- Proteção autônoma contra ransomware (ARP) Para volumes FlexGroup, incluindo a seguinte funcionalidade suportada:
  - Operações de expansão do FlexGroup: Um novo volume de membro herda atributos de proteção autônoma contra ransomware.
  - Conversões de FlexVol para FlexGroup: É possível conversões de FlexVols com proteção ativa autônoma contra ransomware.
  - Rebalanceamento do FlexGroup: A proteção autônoma contra ransomware é suportada durante operações de rebalanceamento ininterruptas e sem interrupções.
- Agende uma única operação de rebalanceamento do FlexGroup.
- SnapMirror fanout Relações com o SVM DR em FlexGroup volumes. Suporta fanout para oito sites.

Recursos suportados começando com ONTAP 9.12,1

- Rebalanceamento do FlexGroup
- SnapLock para SnapVault
- FabricPool, FlexGroup e SVM DR trabalhando em conjunto. (Em versões anteriores ao ONTAP 9.12,1, quaisquer dois desses recursos funcionaram juntos, mas não todos os três em conjunto.)
- Suporte de grande volume Aumenta o tamanho do membro do volume FlexGroup de um máximo de 100TB para um máximo de 300TB.

Recursos suportados começando com ONTAP 9.11,1

- Volumes SnapLock

  O SnapLock não oferece suporte aos seguintes recursos com o FlexGroup volumes:

  - Guarda legal
  - Retenção baseada em evento
  - SnapLock para SnapVault

Você configura o SnapLock no nível FlexGroup. Você não pode configurar o SnapLock no nível de volume do membro.

- Eliminação do diretório assíncrono do cliente

Recursos suportados começando com ONTAP 9.10,1

- Converta um FlexVol volume em um volume FlexGroup em uma relação do SVM DR
- SVM DR FlexClone compatível com FlexGroup volumes

Recursos suportados começando com ONTAP 9.9,1

- Recuperação de desastres da SVM

  Clonar um volume de FlexGroup que faz parte da relação do SVM DR não é compatível.

- Relações de fanout de SnapMirror de 2 ou mais (A A B, A a C), com um máximo de 8 pernas de fanout.

  Considerações para criar relações de cascata e fanout do SnapMirror para FlexGroups

- Relacionamentos em cascata do SnapMirror até dois níveis (A A B a C)

  Considerações para criar relações de cascata e fanout do SnapMirror para FlexGroups

Recursos suportados começando com ONTAP 9.8

- Restaurando um único arquivo de um cofre do FlexGroup SnapMirror ou de um destino UDP
  - A restauração pode ser de um volume FlexGroup de qualquer geometria para o volume FlexGroup de qualquer geometria
  - Apenas um arquivo por operação de restauração é suportado
- Conversão de volumes transferidos de sistemas 7-Mode para volumes FlexGroup

Para obter mais informações, consulte o artigo da base de dados de Conhecimento "Como converter um FlexVol transicionado para FlexGroup".

- NFSv4.2
- Eliminação assíncrona de ficheiros e diretórios
- Análise do sistema de arquivos (FSA)
- FlexGroup como um armazenamento de dados do VMware vSphere
- Suporte adicional para backup e restauração de fita usando NDMP, incluindo os seguintes recursos:
  - Extensão de backup NDMP restartable (RBE) e extensão de gerenciamento de Snapshot (SSME)
  - Variáveis de ambiente EXCLUEM e MULTI_SUBTREE_NAMES suportam backups FlexGroup
  - Introdução da variável de ambiente IGNORE_CTIME_MTIME para backups do FlexGroup
  - Recuperação de arquivos individuais em um FlexGroup usando a mensagem NDMP_SNAP_RECOVER, que faz parte da extensão 0x2050 as sessões de despejo e restauração são abortadas durante uma atualização ou reversão.

Recursos suportados começando com ONTAP 9.7

- Volume FlexClone
- NFSv4 e NFSv4.1
- PNFS
- Backup e restauração em fita usando NDMP

  Você precisa estar ciente dos seguintes pontos para obter suporte NDMP no FlexGroup volumes:

  - A mensagem NDMP_snap_RECOVER na classe de extensão 0x2050 pode ser usada apenas para recuperar um volume FlexGroup inteiro.

    Arquivos individuais em um volume FlexGroup não podem ser recuperados.

  - A extensão de backup reiniciável (RBE) do NDMP não é compatível com volumes FlexGroup.
  - As variáveis de ambiente EXCLUEM e MULTI_SUBTREE_NAMES não são suportadas para volumes FlexGroup.
  - O `ndmpcopy` comando é suportado para transferência de dados entre volumes FlexVol e FlexGroup.

    Se você reverter do Data ONTAP 9,7 para uma versão anterior, as informações de transferência incremental das transferências anteriores não serão mantidas e, portanto, você deverá executar uma cópia de linha de base após a reversão.

- VMware vStorage APIs para Array Integration (VAAI)
- Conversão de um FlexVol volume para um volume FlexGroup
- Volumes FlexGroup como volumes de origem FlexCache

Recursos suportados começando com ONTAP 9.6

- Compartilhamentos SMB continuamente disponíveis
- "Configurações do MetroCluster"
- Renomeando um comando volume FlexGroup(`volume rename`)

- Reduzir ou reduzir o tamanho de um comando FlexGroup volume(`volume size`)
- Dimensionamento elástico
- Criptografia de agregados NetApp (NAE)
- Cloud Volumes ONTAP

Recursos suportados começando com ONTAP 9.5

- Descarga de cópia ODX
- Proteção de acesso no nível de storage
- Melhorias para alterar notificações para compartilhamentos SMB

  As notificações de mudança são enviadas para alterações no diretório pai no qual a `changenotify` propriedade está definida e para alterações em todos os subdiretórios nesse diretório pai.

- FabricPool
- Aplicação das quotas
- Estatísticas Qtree
- QoS adaptável para arquivos em volumes FlexGroup
- FlexCache (apenas cache; FlexGroup como origem suportado no ONTAP 9.7)

Recursos suportados começando com ONTAP 9.4

- FPolicy
- Auditoria de arquivos
- Piso de taxa de transferência (QoS min) e QoS adaptável para volumes FlexGroup
- Limite máximo de taxa de transferência (QoS máx.) e piso de taxa de transferência (QoS min) para arquivos em volumes FlexGroup

  Use o `volume file modify` comando para gerenciar o grupo de políticas de QoS associado a um arquivo.

- Relaxed SnapMirror Limits
- SMB 3.x multicanal

Recursos suportados começando com ONTAP 9.3

- Configuração antivírus
- Alterar notificações para compartilhamentos SMB

  As notificações são enviadas apenas para alterações no diretório pai no qual a `changenotify` propriedade está definida. As notificações de mudança não são enviadas para alterações nos subdiretórios no diretório pai.

- Qtrees
- Limite máximo de taxa de transferência (QoS máx.)
- Expanda o volume do FlexGroup de origem e o volume do FlexGroup de destino em uma relação do SnapMirror

- Backup e restauração do SnapVault
- Relacionamentos unificados de proteção de dados
- Opção de crescimento automático e opção de retração automática
- Contagem de inodes fatorada para ingestão

Recurso suportado a partir de ONTAP 9.2

- Criptografia de volumes
- Deduplicação in-line de agregado (deduplicação entre volumes)
- Criptografia de volume NetApp (NVE)

Recursos suportados começando com ONTAP 9.1

Os volumes do FlexGroup foram introduzidos no ONTAP 9.1, com suporte para vários recursos do ONTAP.

- Tecnologia SnapMirror
- Cópias Snapshot
- Consultor digital
- Compactação adaptável in-line
- Deduplicação in-line
- Compactação de dados in-line
- AFF
- Relatórios de cota
- Tecnologia NetApp Snapshot
- Software SnapRestore (nível FlexGroup)
- Agregados híbridos
- Movimento do volume do componente ou do membro
- Deduplicação pós-processo
- Tecnologia NetApp RAID-TEC
- Ponto de consistência por agregado
- Compartilhando o FlexGroup com o FlexVol volume no mesmo SVM

Configurações de volume FlexGroup não suportadas no ONTAP 9

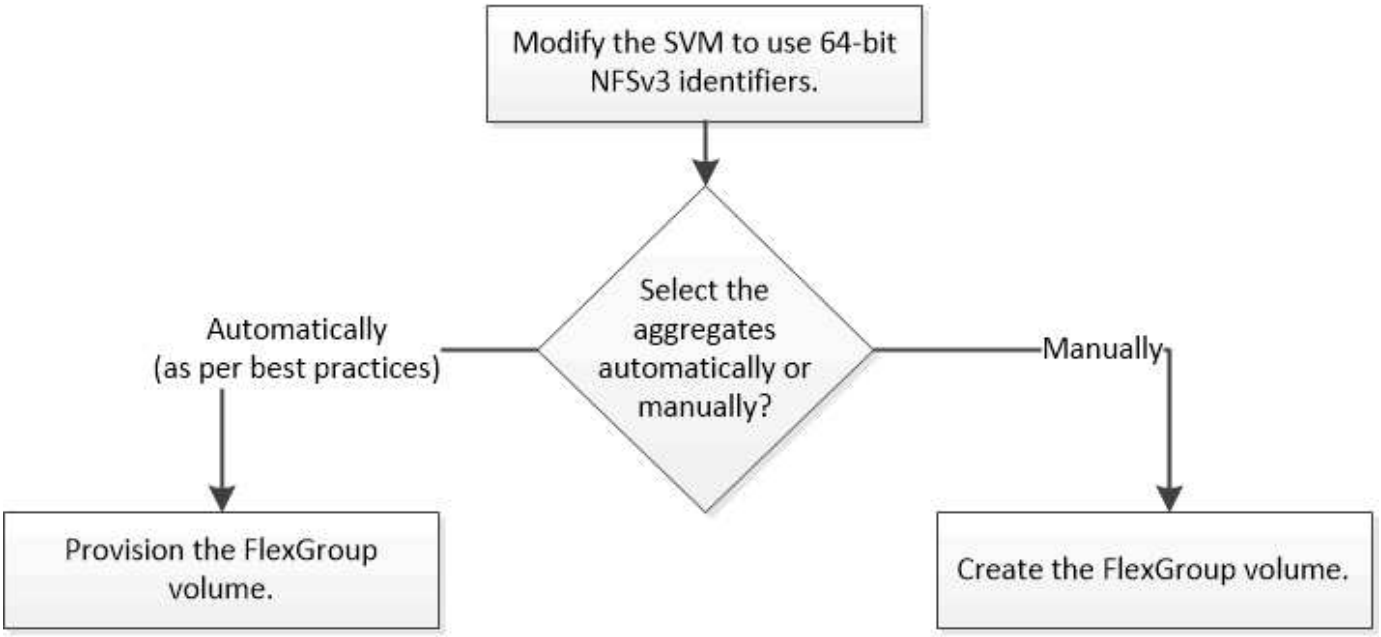
Protocolos não suportados	Recursos de proteção de dados não suportados	Outras funcionalidades do ONTAP não suportadas

• PNFS (ONTAP 9 .6 e anteriores) • SMB 1,0 • Failover transparente para SMB (ONTAP 9.5 e anteriores) • SAN	• Volumes SnapLock (ONTAP 9.10,1 e anteriores) • SMTape • SnapMirror síncrono • SVM DR com volumes FlexGroup que contêm FabricPools (ONTAP 9.11,1 e versões anteriores)	• Serviço de cópia de sombra de volume remoto (VSS) • Mobilidade de dados do SVM

Configuração do volume FlexGroup

Fluxo de trabalho de configuração do volume FlexGroup

Você pode provisionar um volume FlexGroup no qual o ONTAP seleciona automaticamente os agregados com base nas práticas recomendadas para performance ideal ou criar um volume FlexGroup selecionando manualmente os agregados e configurando-o para acesso aos dados.



O que você vai precisar

Você precisa ter criado o SVM com NFS e SMB adicionado à lista de protocolos permitidos para o SVM.

Sobre esta tarefa

Você pode provisionar automaticamente um volume FlexGroup somente em clusters com quatro nós ou menos. Em clusters com mais de quatro nós, você precisa criar um volume FlexGroup manualmente.

Habilite identificadores NFSv3 de 64 bits em um SVM

Para oferecer suporte à alta contagem de arquivos de volumes FlexGroup e evitar colisões de ID de arquivo, você deve habilitar identificadores de arquivo de 64 bits no SVM no qual o volume FlexGroup deve ser criado.

Passos

1. Inicie sessão no nível de privilégio avançado: `set -privilege advanced`
2. Modifique o SVM para usar FSIDs NFSv3 de 64 bits e IDs de arquivo: `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
         FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
         result in older client software no longer working with the
volumes
         owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
         "vs0", it is highly recommended that you remount all NFSv3
clients
         connected to it after the command completes.
Do you want to continue? {y|n}: y
```

Depois de terminar

Todos os clientes devem ser remontados. Isso é necessário porque as IDs do sistema de arquivos mudam e os clientes podem receber mensagens de manipulação de arquivos obsoletos ao tentar operações NFS.

Provisionar um volume FlexGroup automaticamente

Ao criar um volume FlexGroup, você pode optar por que o ONTAP provisione automaticamente o volume FlexGroup selecionando os agregados. Os agregados são selecionados com base nas práticas recomendadas para desempenho e capacidade ideais.

Antes de começar

Cada nó no cluster deve ter pelo menos um agregado.

> Para criar um volume FlexGroup para FabricPool no ONTAP 9.5, cada nó deve ter pelo menos um agregado que seja o FabricPool.

Sobre esta tarefa

O ONTAP seleciona dois agregados com a maior quantidade de espaço utilizável em cada nó para criar o volume FlexGroup. Se dois agregados não estiverem disponíveis, o ONTAP selecionará um agregado por nó para criar o volume FlexGroup.

A partir do ONTAP 9.15,1, quando você provisiona automaticamente um volume FlexGroup, o ONTAP usa o

posicionamento balanceado (BP) para escolher os agregados e o layout do componente FlexGroup. Um aspeto da BP é como ela limita o provisionamento excessivo de agregados ao criar volumes FlexGroup garantidos "nenhum". O tamanho do volume FlexGroup global é limitado pela quantidade de espaço livre nos agregados, embora o limite seja maior do que para volumes FlexGroup garantidos por "volume". Quando você cria um volume FlexGroup usando APIs REST ou `auto-provision-as` com a CLI do ONTAP, o provisionamento pode falhar devido ao espaço insuficiente devido a esse limite. Você pode evitar isso criando volumes FlexGroup menores ou "Criando um volume FlexGroup e selecionando os agregados manualmente"usando o `aggr-list` parâmetro.

Passos

1. Provisione o volume FlexGroup:

Se você estiver usando…	Use este comando…

ONTAP 9 .2 ou posterior	`volume create -vserver svm_name -volume fg_vol_name -auto-provision-as flexgroup -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name] [-support-tiering true]` A partir do ONTAP 9.5, você pode criar volumes do FlexGroup para FabricPool. Para provisionar automaticamente um volume FlexGroup no FabricPool, você deve definir o `-support -tiering` parâmetro como `true`. A garantia de volume deve estar sempre definida como `none` para FabricPool. Você também pode especificar a política de disposição em categorias e o período mínimo de resfriamento de disposição em camadas para o volume FlexGroup. "Gerenciamento de disco e agregado" A partir do ONTAP 9.3, é possível especificar um limite máximo de taxa de transferência (QoS máximo) para volumes FlexGroup, o que limita os recursos de performance que o volume FlexGroup pode consumir. A partir do ONTAP 9.4, é possível especificar andares de taxa de transferência (QoS min) e QoS adaptável para volumes FlexGroup. "Gerenciamento de desempenho" A partir do ONTAP 9.2, pode definir o `-encrypt` parâmetro para `true` se pretender ativar a encriptação no volume FlexGroup. Para criar um volume criptografado, você deve ter instalado a licença de criptografia de volume e o gerenciador de chaves. Você deve habilitar a criptografia em volumes FlexGroup no momento da criação. Não é possível ativar a encriptação em volumes FlexGroup existentes. "Criptografia de dados em repouso"
ONTAP 9,1	`volume flexgroup deploy -vserver svm_name -size fg_size`

O `size` parâmetro especifica o tamanho do volume FlexGroup em KB, MB, GB, TB ou PB.

O exemplo a seguir mostra como provisionar um volume FlexGroup de tamanho 400 TB no ONTAP 9.2:

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

O exemplo a seguir mostra como criar um grupo de políticas de QoS para limite de taxa de transferência e como aplicá-lo a um volume FlexGroup:

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

O exemplo a seguir mostra como provisionar um volume FlexGroup de tamanho 400 TB em agregados no FabricPool no ONTAP 9.5:

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

O volume FlexGroup é criado com oito componentes em cada nó no cluster. Os constituintes são distribuídos igualmente entre os dois maiores agregados em cada nó.

Por padrão, o volume FlexGroup é criado com a `volume` configuração de garantia de espaço, exceto em sistemas AFF. Para sistemas AFF, por padrão, o volume FlexGroup é criado com a `none` garantia de espaço.

2. Monte o volume FlexGroup com um caminho de junção: `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

Depois de terminar

Você deve montar o volume FlexGroup do cliente.

Se você estiver executando o ONTAP 9.6 ou anterior e se a máquina virtual de armazenamento (SVM) tiver o NFSv3 e o NFSv4 configurados, a montagem do volume FlexGroup do cliente poderá falhar. Nesses casos, você deve especificar explicitamente a versão NFS ao montar o volume FlexGroup do cliente.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

Crie um volume FlexGroup

Você pode criar um volume FlexGroup selecionando manualmente os agregados nos quais o volume FlexGroup deve ser criado e, em seguida, especificando o número de constituintes em cada agregado.

Sobre esta tarefa

Você precisa estar ciente do espaço necessário nos agregados para criar um volume FlexGroup.

Você deve considerar as seguintes diretrizes ao criar um volume FlexGroup para obter os melhores resultados de desempenho com um volume FlexGroup:

- Um volume FlexGroup deve abranger apenas agregados que estejam em sistemas de hardware idênticos.

  O uso de sistemas de hardware idênticos ajuda a fornecer desempenho previsível em todo o volume FlexGroup.

- Um volume FlexGroup deve abranger agregados com o mesmo tipo de disco e configurações de grupo RAID.

  Para uma performance consistente, você precisa garantir que todos os agregados sejam compostos por todos os SSDs, todos os HDDs ou todos os agregados híbridos. Além disso, os agregados devem ter o mesmo número de unidades e grupos RAID no volume FlexGroup.

- Um volume FlexGroup pode abranger partes de um cluster.

  Um volume FlexGroup não precisa ser configurado para abranger todo o cluster, mas isso pode aproveitar ainda mais os recursos de hardware disponíveis.

- Ao criar um volume FlexGroup, é melhor se os agregados nos quais o volume FlexGroup é implantado tiverem as seguintes caraterísticas:
  - Aproximadamente a mesma quantidade de espaço livre deve estar disponível em vários agregados, especialmente ao usar thin Provisioning.

- Aproximadamente 3% do espaço livre deve ser reservado para metadados agregados após a criação do volume FlexGroup.

- Para sistemas FAS, é melhor ter dois agregados por nó e, para sistemas AFF, você precisa ter um agregado por nó para o volume FlexGroup.
- Para cada volume FlexGroup, você deve criar pelo menos oito componentes distribuídos em dois ou mais agregados em sistemas FAS e em um ou mais agregados em sistemas AFF.

Antes de começar

- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Criar o volume FlexGroup: `volume create -vserver svm_name -volume flexgroup_name -aggr-list aggr1,aggr2,.. -aggr-list-multiplier constituents_per_aggr -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name]`

   - O `-aggr-list` parâmetro especifica a lista de agregados a serem usados para componentes de volume FlexGroup.

     Cada entrada na lista cria um constituinte no agregado especificado. Você pode especificar um agregado várias vezes para ter vários constituintes criados no agregado.

     Para obter performance consistente em todo o volume FlexGroup, todos os agregados precisam usar o mesmo tipo de disco e configurações de grupo RAID.

   - O `-aggr-list-multiplier` parâmetro especifica o número de vezes a iterar sobre os agregados que são listados com o `-aggr-list` parâmetro ao criar um volume FlexGroup.

     O valor padrão do `-aggr-list-multiplier` parâmetro é 4.

   - O `size` parâmetro especifica o tamanho do volume FlexGroup em KB, MB, GB, TB ou PB.
   - A partir do ONTAP 9.5, é possível criar volumes FlexGroup para FabricPool, que usam apenas todos os agregados SSD.

     Para criar um volume FlexGroup para FabricPool, todos os agregados especificados com o `-aggr-list` parâmetro devem ser FabricPool. A garantia de volume deve estar sempre definida como `none` para FabricPool. Você também pode especificar a política de disposição em categorias e o período mínimo de resfriamento de disposição em camadas para o volume FlexGroup.

     Gerenciamento de disco e agregado

   - A partir do ONTAP 9.4, é possível especificar andares de taxa de transferência (QoS min) e QoS adaptável para volumes FlexGroup.

     "Gerenciamento de desempenho"

   - A partir do ONTAP 9.3, é possível especificar um limite máximo de taxa de transferência (QoS máximo) para volumes FlexGroup, o que limita os recursos de performance que o volume FlexGroup

pode consumir.

- A partir do ONTAP 9.2, pode definir o `-encrypt` parâmetro para `true` se pretender ativar a encriptação no volume FlexGroup.

  Para criar um volume criptografado, você deve ter instalado a licença de criptografia de volume e o gerenciador de chaves.

  > Você deve habilitar a criptografia em volumes FlexGroup no momento da criação. Não é possível ativar a encriptação em volumes FlexGroup existentes.

  "Criptografia de dados em repouso"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number of
constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

No exemplo anterior, se você quiser criar o volume FlexGroup para FabricPool, todos os agregados (aggr1, aggr2 e aggr3) devem ser agregados no FabricPool. Monte o volume FlexGroup com um caminho de junção: `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

Depois de terminar

Você deve montar o volume FlexGroup do cliente.

Se você estiver executando o ONTAP 9.6 ou anterior e se a máquina virtual de armazenamento (SVM) tiver o NFSv3 e o NFSv4 configurados, a montagem do volume FlexGroup do cliente poderá falhar. Nesses casos, você deve especificar explicitamente a versão NFS ao montar o volume FlexGroup do cliente.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

Informações relacionadas

"Relatório técnico da NetApp 4571: Guia de práticas recomendadas e implementação da NetApp FlexGroup"

Gerenciar o FlexGroup volumes

Monitore o uso de espaço de um volume FlexGroup

Você pode visualizar um volume FlexGroup e seus constituintes e monitorar o espaço usado pelo volume FlexGroup.

Sobre esta tarefa

Começando com ONTAP 9.6, o dimensionamento elástico é suportado. O ONTAP aumenta automaticamente um componente de um volume FlexGroup se ele estiver ficando sem espaço, reduzindo qualquer outro componente no volume FlexGroup que tenha espaço livre em uma quantidade equivalente. O dimensionamento elástico evita erros de espaço que são gerados devido a um ou mais volumes constituintes do FlexGroup que ficam sem espaço.

> A partir do ONTAP 9.9,1, relatórios de espaço lógico e imposição também estão disponíveis para volumes FlexGroup. Para obter mais informações, "Relatórios de espaço lógico e imposição para volumes"consulte .

Passo

1. Veja o espaço utilizado pelo volume FlexGroup e seus componentes: `volume show -vserver vserver_name -volume-style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1          -            online     RW        500GB
207.5GB   56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1__0001    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0002    aggr1        online     RW      31.25GB
12.98GB   56%
vs1       fg1__0003    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0004    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0005    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0006    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0007    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0008    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0009    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0010    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0011    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0012    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0013    aggr3        online     RW      31.25GB
12.95GB   56%
vs1       fg1__0014    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0015    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0016    aggr1        online     RW      31.25GB
13.01GB   56%
16 entries were displayed.
```

Você pode usar o espaço disponível e o espaço percentual usado para monitorar o uso do espaço do volume FlexGroup.

Aumente o tamanho de um volume FlexGroup

Você pode aumentar o tamanho de um volume FlexGroup adicionando mais capacidade aos volumes membros (constituintes) existentes do volume FlexGroup ou expandindo o volume FlexGroup com novos volumes membros. Um volume FlexGroup não pode ter mais de 200 volumes de membros.

Antes de começar

Espaço suficiente deve estar disponível nos agregados.

Sobre esta tarefa

Se você quiser adicionar mais espaço, você pode aumentar o tamanho coletivo do volume FlexGroup. Aumentar o tamanho de um volume FlexGroup redimensiona os volumes de membros existentes do volume FlexGroup.

Se você quiser melhorar o desempenho, pode expandir o volume FlexGroup. Você pode querer expandir um volume do FlexGroup e adicionar novos volumes de membros nas seguintes situações:

- Novos nós foram adicionados ao cluster.
- Novos agregados foram criados nos nós existentes.
- Os volumes de membros existentes do volume FlexGroup atingiram o tamanho máximo de FlexVol para o hardware (100TB ou 300TB se "suporte de grande volume" tiver sido ativado) e, portanto, o volume FlexGroup não pode ser redimensionado sem adicionar volumes de membros adicionais.

Em versões anteriores ao ONTAP 9.3, não é possível expandir volumes do FlexGroup depois que um relacionamento do SnapMirror for estabelecido. Se você expandir o volume FlexGroup de origem depois de quebrar a relação SnapMirror em versões anteriores ao ONTAP 9.3, será necessário realizar uma transferência de linha de base para o volume FlexGroup de destino novamente. A partir do ONTAP 9.3, é possível expandir volumes do FlexGroup que estão em uma relação do SnapMirror.

Passo

1. Aumente o tamanho do volume FlexGroup aumentando a capacidade ou a performance do volume FlexGroup, conforme necessário:

Se você quiser aumentar a…	Então faça isso…
Capacidade do volume FlexGroup	Redimensione os volumes de membros do volume FlexGroup: `volume modify -vserver vserver_name -volume fg_name -size new_size`

Desempenho para o volume FlexGroup	Expanda o volume FlexGroup adicionando novos volumes de membros (constituintes): `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]` O valor padrão do `-aggr-list-multiplier` parâmetro é 1. Para expandir um volume FlexGroup para FabricPool no ONTAP 9.5, todos os novos agregados usados devem ser FabricPool.

Sempre que possível, você deve aumentar a capacidade de um volume FlexGroup. Se for necessário expandir um volume FlexGroup, adicione volumes de membros nas mesmas múltiplas que os volumes de membros do volume FlexGroup existente para garantir uma performance consistente. Por exemplo, se o volume FlexGroup existente tiver 16 volumes membros com oito volumes membros por nó, você poderá expandir o volume FlexGroup existente em 8 ou 16 volumes membros.

Exemplos

Exemplo de aumento da capacidade dos volumes de membros existentes

O exemplo a seguir mostra como adicionar espaço de 20 TB a um volX de volume FlexGroup:

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

Se o volume FlexGroup tiver 16 volumes de membros, o espaço de cada volume de membro será aumentado em 1,25 TB.

Exemplo de melhoria do desempenho adicionando novos volumes de membros

O exemplo a seguir mostra como adicionar mais dois volumes de membros ao volume volX do FlexGroup:

```
cluster1::> volume expand -vserver vs1 -volume volX -aggr-list aggr1,aggr2
```

O tamanho dos novos volumes de membros é o mesmo dos volumes de membros existentes.

Reduza o tamanho de um volume FlexGroup

A partir do ONTAP 9.6, é possível redimensionar um volume FlexGroup para um valor menor do que o tamanho atual para liberar o espaço não utilizado do volume. Quando você reduz o tamanho de um volume FlexGroup, o ONTAP redimensiona automaticamente todos os componentes do FlexGroup.

Passo

1. Verifique o tamanho atual do volume do FlexGroup: 'Tamanho do volume -vserver *vserver_name* -volume

fg_name'

2. Reduza o tamanho do volume FlexGroup: `volume size -vserver` *`vserver_name`* `-volume` *`fg_name new_size`*

   Quando você especifica o novo tamanho, você pode especificar um valor menor do que o tamanho atual ou um valor negativo usando o sinal de menos (-) pelo qual o tamanho atual do volume FlexGroup é reduzido.

   > Se a redução automática estiver ativada para o comando volume(`volume autosize`), o dimensionamento mínimo será definido para o novo tamanho do volume.

   O exemplo a seguir exibe o tamanho do volume atual do volume FlexGroup chamado volX e redimensiona o volume para 10TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

   O exemplo a seguir exibe o tamanho do volume atual para o volume FlexGroup chamado volX e reduz o tamanho do volume em 5TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

Configure os volumes do FlexGroup para aumentar e diminuir automaticamente o tamanho

A partir do ONTAP 9.3, você pode configurar volumes FlexGroup para aumentar e diminuir automaticamente de acordo com a quantidade de espaço que eles atualmente exigem.

O que você vai precisar

O volume FlexGroup deve estar online.

Sobre esta tarefa

É possível dimensionar volumes FlexGroup em dois modos:

- Aumentar o tamanho do volume automaticamente(`grow`)

O crescimento automático ajuda a evitar que um volume de FlexGroup fique sem espaço, se o agregado puder fornecer mais espaço. Pode configurar o tamanho máximo para o volume. O aumento é acionado automaticamente com base na quantidade de dados que estão sendo gravados no volume em relação à quantidade atual de espaço usado e quaisquer limites definidos.

Por padrão, o tamanho máximo para o qual um volume pode crescer é de 120% do tamanho no qual o crescimento automático é ativado. Se você precisar garantir que o volume pode crescer para ser maior do que isso, você deve definir o tamanho máximo para o volume de acordo.

- Reduzir o tamanho do volume automaticamente(`grow_shrink`)

  O encolhimento automático impede que um volume seja maior do que o necessário, liberando espaço no agregado para uso por outros volumes.

  O Autoshink só pode ser usado em combinação com o crescimento automático para atender às demandas de espaço em constante mudança e não está disponível sozinho. Quando a opção Autoshink está ativada, o ONTAP gerencia automaticamente o comportamento de encolhimento de um volume para evitar um ciclo infinito de ações com crescimento automático e com redução automática.

À medida que um volume aumenta, o número máximo de arquivos que ele pode conter pode ser aumentado automaticamente. Quando um volume é reduzido, o número máximo de arquivos que ele pode conter permanece inalterado e um volume não pode ser encolhido automaticamente abaixo do tamanho que corresponde ao número máximo de arquivos atual. Por esse motivo, pode não ser possível reduzir automaticamente um volume até o tamanho original.

Passo

1. Configure o volume para crescer e diminuir seu tamanho automaticamente: `volume autosize -vserver vserver_name -volume vol_name -mode [grow | grow_shrink]`

   Você também pode especificar o tamanho máximo, o tamanho mínimo e os limites para aumentar ou diminuir o volume.

   O comando a seguir habilita alterações automáticas de tamanho para um volume chamado FG1. O volume é configurado para crescer até um tamanho máximo de 5 TB quando está 70% cheio.

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

Exclua diretórios de forma assíncrona no cluster

A partir do ONTAP 9.8, você pode usar a funcionalidade de exclusão assíncrona para excluir diretórios de compartilhamentos de clientes Linux e Windows de forma assíncrona (ou seja, em segundo plano). Os administradores de cluster e SVM podem executar operações de exclusão assíncrona no FlexVol e no FlexGroup volumes.

Se você estiver usando uma versão do ONTAP anterior ao ONTAP 9.11,1, será necessário ser um administrador de cluster ou um administrador SVM usando o modo de privilégio avançado.

A partir do ONTAP 9.11,1, um administrador de storage pode conceder direitos em um volume para permitir

que clientes NFS e SMB realizem operações de exclusão assíncrona. Para obter mais informações, "Gerencie os direitos do cliente para excluir diretórios assincronamente"consulte .

A partir do ONTAP 9.8, você pode usar a funcionalidade de exclusão assíncrona usando a CLI do ONTAP. A partir do ONTAP 9.9,1, você pode usar essa funcionalidade com o Gerenciador do sistema. Para obter mais informações sobre esse processo, "Tome medidas corretivas com base em análises"consulte .

System Manager

1. Clique em **Storage > volumes** e, em seguida, clique em **Explorer**.

   Quando você passa o Mouse sobre um arquivo ou pasta, a opção para excluir é exibida. Você só pode excluir um objeto de cada vez.

   Quando diretórios e arquivos são excluídos, os novos valores de capacidade de armazenamento não são exibidos imediatamente.

CLI

Use a CLI para executar uma exclusão assíncrona

1. Entrar no modo de privilégio avançado:

   ```
   -privilege advance
   ```

2. Excluir diretórios em um volume FlexVol ou FlexGroup:

   ```
   volume file async-delete start -vserver vserver_name -volume volume_name
   -path file_path -throttle throttle
   ```

   O valor mínimo do acelerador é 10, o máximo é 100.000 e o padrão é 5000.

   O exemplo a seguir exclui o diretório chamado D2, que está localizado no diretório chamado D1.

   ```
   cluster::*>volume file async-delete start -vserver vs1 -volume vol1
   -path d1/d2
   ```

3. Verifique se o diretório foi excluído:

   ```
   event log show
   ```

   O exemplo a seguir mostra a saída para o log de eventos quando o diretório é excluído com sucesso.

   ```
   cluster-cli::*> event log show
   Time                 Node             Severity      Event
   -------------------  ---------------- -------------
   --------------------
   MM/DD/YYYY 00:11:11  cluster-vsim     INFORMATIONAL
   asyncDelete.message.success: Async delete job on path d1/d2 of
   volume (MSID: 2162149232) was completed.
   ```

Cancelar um trabalho de exclusão de diretório

1. Entrar no modo de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Verifique se a exclusão do diretório está em andamento:

   ```
   volume file async-delete show
   ```

   Se o SVM, volume, JobID e caminho do diretório forem exibidos, você poderá cancelar o trabalho.

3. Cancelar a exclusão do diretório:

   ```
   volume file async-delete cancel -vserver SVM_name -volume volume_name
   -jobid job_id
   ```

Gerencie os direitos do cliente para excluir diretórios assincronamente

A partir do ONTAP 9.11,1, os administradores de storage podem conceder direitos sobre um volume para permitir que clientes NFS e SMB realizem operações de exclusão assíncrona. Quando a eliminação assíncrona está ativada no cluster, os utilizadores de clientes Linux podem utilizar o `mv` comando e os utilizadores de clientes Windows podem utilizar o `rename` comando para eliminar um diretório no volume especificado, movendo-o para um diretório oculto que, por predefinição, é chamado .ontaptrashbin.

Ativar a eliminação do diretório assíncrono do cliente

Passos

1. A partir da CLI do cluster, entre no modo de privilégio avançado: `-privilege advance`
2. Ative a exclusão assíncrona do cliente e, se desejado, forneça um nome alternativo para o diretório de trashbin:

   ```
   volume file async-delete client enable volume volname vserver vserverName
   trashbinname name
   ```

   Exemplo usando o nome padrão da lixeira:

   ```
   cluster1::*> volume file async-delete client enable -volume v1 -vserver
   vs0

   Info: Async directory delete from the client has been enabled on volume
   "v1" in
         Vserver "vs0".
   ```

   Exemplo especificando um nome alternativo de lixeira:

```
cluster1::*> volume file async-delete client enable -volume test
-trashbin .ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
      Vserver "vs0".
```

3. Verifique se a exclusão assíncrona do cliente está ativada:

   `volume file async-delete client show`

   Exemplo:

```
cluster1::*> volume file async-delete client show

Vserver Volume      async-delete client TrashBinName
------------ ------------ ---------------------- -------------
vs1          vol1         Enabled          .ntaptrash
vs2          vol2         Disabled          -

2 entries were displayed.
```

Desative a exclusão do diretório assíncrono do cliente

Passos

1. A partir da CLI do cluster, desative a exclusão do diretório asycronic do cliente:

   `volume file async-delete client disable volume` *volname* `vserver` *vserverName*

   Exemplo:

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

       Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. Verifique se a exclusão assíncrona do cliente está desativada:

   `volume file async-delete client show`

   Exemplo:

```
cluster1::*> volume file async-delete client show

Vserver      Volume      async-delete client      TrashBinName
------------ ------------ ---------------------- -------------
vs1          vol1         Disabled                -
vs2          vol2         Disabled                -

2 entries were displayed.
```

Crie qtrees com volumes FlexGroup

Começando com ONTAP 9.3, você pode criar qtrees com volumes FlexGroup. Qtrees permitem que você particione seus volumes FlexGroup em segmentos menores que você pode gerenciar individualmente.

Sobre esta tarefa

- Se o volume FlexGroup de origem tiver qtrees em uma relação SnapMirror, o cluster de destino deve estar executando o ONTAP 9.3 ou posterior (uma versão do software ONTAP que suporta qtrees).
- A partir do ONTAP 9.5, as estatísticas de qtree são suportadas para volumes FlexGroup.

Passos

1. Crie uma qtree no volume FlexGroup:

   ```
   volume qtree create -vserver <vserver_name> -volume <volume_name> -qtree
   <qtree_name>
   ```

   Opcionalmente, você pode especificar o estilo de segurança, os princípios SMB, as permissões UNIX e a política de exportação para a qtree.

   ```
   cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1
   -security-style mixed
   ```

Informações relacionadas

"Gerenciamento de storage lógico"

Usar cotas para volumes FlexGroup

No ONTAP 9.4 e versões anteriores, você pode aplicar regras de cotas aos volumes do FlexGroup apenas para fins de geração de relatórios, mas não para impor limites de cota. A partir do ONTAP 9.5, é possível impor limites às regras de cota aplicadas aos volumes do FlexGroup.

Sobre esta tarefa

- A partir do ONTAP 9.5, é possível especificar cotas de limite rígido, flexível e de limite de limite para volumes FlexGroup.

  Você pode especificar esses limites para restringir a quantidade de espaço, o número de arquivos que um usuário, grupo ou qtree específico pode criar, ou ambos. Os limites de cota geram mensagens de aviso nos seguintes cenários:

  - Quando o uso excede um limite de software configurado, o ONTAP emite uma mensagem de aviso, mas ainda é permitido tráfego adicional.

    Se a utilização mais tarde descer abaixo do limite de software configurado novamente, é emitida uma mensagem totalmente limpa.

  - Quando o uso excede um limite de limite configurado, o ONTAP emite uma segunda mensagem de aviso.

    Nenhuma mensagem administrativa totalmente clara é emitida quando o uso mais tarde cai abaixo de um limite de limite configurado.

  - Se a utilização atingir um limite rígido configurado, o ONTAP impede o consumo adicional de recursos rejeitando o tráfego.
- No ONTAP 9.5, as regras de quota não podem ser criadas ou ativadas no volume FlexGroup de destino de uma relação SnapMirror.
- Durante a inicialização da cota, as cotas não são aplicadas e não há notificações de cotas violadas após a inicialização da cota.

  Para verificar se as cotas foram violadas durante a inicialização da cota, você pode usar o `volume quota report` comando.

Cotas e tipos

As cotas têm um tipo: Podem ser usuário, grupo ou árvore. Os alvos de cota especificam o usuário, grupo ou qtree para o qual os limites de cota são aplicados.

A tabela a seguir lista os tipos de metas de cota, os tipos de cotas a que cada meta de cota está associada e como cada meta de cota é representada:

Destino de cota	Tipo de cota	Como o alvo é representado	Notas
utilizador	quota de utilizador	Nome de utilizador UNIX UID UNIX Nome de utilizador do Windows no formato pré-Windows 2000 Windows SID	As cotas de usuário podem ser aplicadas para um volume ou qtree específico.

grupo	cota de grupo	Nome do grupo UNIX GID	As cotas de grupo podem ser aplicadas para um volume ou qtree específico. O ONTAP não aplica cotas de grupo com base em IDs do Windows.
qtree	cota de árvore	nome de qtree	As cotas de árvore são aplicadas a um volume específico e não afetam qtrees em outros volumes.
""	cota de usuário quotagroup cota de árvore	Aspas duplas (""")	Um alvo de cota de "" denota uma quota *default*. Para cotas padrão, o tipo de cota é determinado pelo valor do campo tipo.

Comportamento dos volumes FlexGroup quando os limites de cota são excedidos

A partir do ONTAP 9.5, os limites de cota são suportados em volumes FlexGroup. Existem algumas diferenças na forma como os limites de cota são aplicados em um volume FlexGroup quando comparado a um FlexVol volume.

Os volumes FlexGroup podem mostrar os seguintes comportamentos quando os limites de cota são excedidos:

- O espaço e o uso de arquivos em um volume FlexGroup podem atingir até 5% mais alto do que o limite rígido configurado antes que o limite de cota seja imposto pela rejeição de tráfego adicional.

  Para fornecer o melhor desempenho, o ONTAP pode permitir que o consumo de espaço exceda o limite rígido configurado por uma pequena margem antes do início da aplicação da cota. Esse consumo de espaço adicional não excede 5% dos limites rígidos configurados, 1 GB ou 65536 arquivos, o que for menor.

- Depois que o limite de cota for atingido, se um usuário ou administrador excluir alguns arquivos ou diretórios de modo que o uso de cota esteja agora abaixo do limite, a operação de arquivo que consome cota subsequente pode retomar com um atraso (pode levar até 5 segundos para ser retomada).
- Quando o espaço total e o uso do arquivo de um volume FlexGroup excederem os limites de cota configurados, pode haver um ligeiro atraso no Registro de uma mensagem de log de eventos.
- Você pode obter erros "sem espaço" se alguns constituintes do volume FlexGroup ficarem cheios, mas os limites de cota não forem atingidos.
- Operações, como renomear um arquivo ou diretório ou mover arquivos entre qtrees, em alvos de cota, para os quais os limites rígidos de cota são configurados, podem levar mais tempo quando comparadas a

operações semelhantes em volumes FlexVol.

Exemplos de aplicação de cotas para volumes FlexGroup

Você pode usar os exemplos para entender como configurar cotas com limites no ONTAP 9.5 e posterior.

Exemplo 1: Aplicando uma regra de cota com limites de disco

1. Você deve criar uma regra de tipo de política de cota `user` com um limite de disco macio alcançável e um limite de disco rígido.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. Você pode exibir a regra de política de cota:

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG

Vserver: vs0               Policy: default           Volume: FG

                                              Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           1TB    800GB       -        -
-
```

3. Para ativar a nova regra de cota, inicialize cotas no volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Você pode exibir as informações de uso de disco e de uso de arquivos do volume FlexGroup usando o relatório de cota.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    root      50GB      -       1       -
FG                 user    *         800GB    1TB      0       -   *
2 entries were displayed.
```

Depois que o limite do disco rígido é atingido, o destino da regra de política de cota (usuário, neste caso) é impedido de gravar mais dados nos arquivos.

Exemplo 2: Aplicar uma regra de quota para vários utilizadores

1. Você deve criar uma regra de política de cota de tipo `user`, em que vários usuários sejam especificados no destino de cota (usuários UNIX, usuários SMB ou uma combinação de ambos) e em que a regra tenha tanto um limite de disco macio quanto um limite de disco rígido alcançáveis.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit  800GB
```

2. Você pode exibir a regra de política de cota:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "rdavis,ABCCORP\RobertDavis"  "" off  1TB  800GB  -  -
```

3. Para ativar a nova regra de cota, inicialize cotas no volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Você pode verificar se o estado da cota está ativo:

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
               Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. Você pode exibir as informações de uso de disco e de uso de arquivos do volume FlexGroup usando o relatório de cota.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis,ABCCORP\RobertDavis
```

O limite de cota é compartilhado entre todos os usuários listados no destino de cota.

Depois que o limite do disco rígido é atingido, os usuários listados no alvo de cota são bloqueados de gravar mais dados nos arquivos.

Exemplo 3: Aplicando a cota com o mapeamento de usuários ativado

1. Você deve criar uma regra de política de cota de tipo `user`, especificar um usuário UNIX ou um usuário do Windows como o destino de cota com `user-mapping` definido como `on`e criar a regra com um limite de disco rígido e um limite de disco rígido alcançáveis.

   O mapeamento entre usuários UNIX e Windows deve ser configurado anteriormente usando o `vserver name-mapping create` comando.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit  800GB -user-mapping on
```

2. Você pode exibir a regra de política de cota:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0              Policy: default           Volume: FG

                                                 Soft             Soft
                        User         Disk        Disk    Files    Files
Type   Target    Qtree  Mapping      Limit       Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   rdavis    ""      on           1TB    800GB       -        -
-
```

3. Para ativar a nova regra de cota, inicialize cotas no volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Você pode verificar se o estado da cota está ativo:

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
                Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. Você pode exibir as informações de uso de disco e de uso de arquivos do volume FlexGroup usando o relatório de cota.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis
```

O limite de cota é compartilhado entre o usuário listado no destino de cota e o usuário correspondente do Windows ou UNIX.

Depois que o limite do disco rígido é atingido, tanto o usuário listado no destino da cota quanto seu usuário correspondente do Windows ou UNIX é impedido de gravar mais dados nos arquivos.

Exemplo 4: Verificando o tamanho de qtree quando a cota está ativada

1. Você deve criar uma regra de política de cota de tipo `tree` e onde a regra tenha um limite de disco flexível alcançável e um limite de disco rígido.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. Você pode exibir a regra de política de cota:

```
cluster1::> quota policy rule show -vserver vs0

Vserver: vs0               Policy: default           Volume: FG

                                              Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   tree_4118314302  "" -          48GB        -      20        -
```

3. Para ativar a nova regra de cota, inicialize cotas no volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

a. Você pode exibir as informações de uso de disco e de uso de arquivos do volume FlexGroup usando o relatório de cota.

```
cluster1::> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
------- -------- ------ ------- ----- ----- ------ ------ ---------
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

O limite de cota é compartilhado entre o usuário listado no destino de cota e o usuário correspondente do Windows ou UNIX.

4. A partir de um cliente NFS, use o `df` comando para visualizar o uso total do espaço, o espaço disponível e o espaço usado.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

Com o limite rígido, o uso do espaço é calculado a partir de um cliente NFS da seguinte forma:

- Uso total de espaço: Limite rígido para árvore
- Espaço livre: Limite rígido menos o uso do espaço de qtree sem limite rígido, o uso do espaço é calculado a partir de um cliente NFS da seguinte forma:
- Uso de espaço: Uso de cota
- Espaço total: Soma do uso da cota e espaço físico livre no volume

5. No compartilhamento SMB, use o Windows Explorer para exibir a utilização total do espaço, o espaço disponível e o espaço usado.

Em um compartilhamento SMB, você deve estar ciente das seguintes considerações para calcular o uso do espaço:

- O limite rígido da quota de utilizador para o utilizador e o grupo é levado em consideração para calcular o espaço total disponível.
- O valor mínimo entre o espaço livre da regra de cota de árvore, a regra de cota de usuário e a regra de cota de grupo é considerado como o espaço livre para o compartilhamento SMB.
- O uso total de espaço é variável para SMB e depende do limite rígido que corresponde ao espaço livre mínimo entre a árvore, o usuário e o grupo.

Aplique regras e limites no volume FlexGroups

Passos

1. Criar regras de quota para alvos : `volume quota policy rule create -vserver vs0 -policy -name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold`

`threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]`

- No ONTAP 9.2 e no ONTAP 9.1, o tipo de destino de cota pode ser somente `user` ou `group` para volumes FlexGroup.

  O tipo de cota de árvore não é suportado para volumes FlexGroup no ONTAP 9.2 e no ONTAP 9.1.

- No ONTAP 9.3 e posterior, o tipo de destino de cota pode ser `user`, `group` ou `tree` para volumes FlexGroup.
- Um caminho não é suportado como destino ao criar regras de cota para volumes FlexGroup.
- A partir do ONTAP 9.5, você pode especificar limite de disco rígido, limite de arquivo rígido, limite de disco flexível, limite de arquivo macio e cotas de limite de limite para volumes FlexGroup.

  No ONTAP 9.4 e anteriores, você não pode especificar o limite de disco, limite de arquivo, limite de disco, limite de disco flexível ou limite de arquivo macio quando você criar regras de cota para volumes FlexGroup.

O exemplo a seguir mostra uma regra de cota padrão que está sendo criada para o tipo de destino do usuário:

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

O exemplo a seguir mostra uma regra de cota de árvore que está sendo criada para a qtree chamada qtree1:

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. Ative as cotas para o volume FlexGroup especificado: `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. Monitorar o estado da inicialização da cota: `volume quota show -vserver svm_name`

Os volumes FlexGroup podem mostrar o `mixed` estado, o que indica que todos os volumes constituintes ainda não estão no mesmo estado.

```
cluster1::> volume quota show -vserver vs0
                                        Scan
Vserver    Volume        State          Status
---------  ------------  -------------  ------
vs0        fg1           initializing       95%
vs0        vol1          off                 -
2 entries were displayed.
```

1. Exibir o relatório de cota para o volume FlexGroup com cotas ativas: `volume quota report -vserver svm_name -volume flexgroup_vol`

   Não é possível especificar um caminho com o `volume quota report` comando para volumes FlexGroup.

   O exemplo a seguir mostra a cota de usuário para o volume FlexGroup FG1:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
  Vserver: vs0
                                       ----Disk----  ----Files-----
Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  fg1                user    *           0B      -       0       -   *
  fg1                user    root       1GB      -       1       -   *
  2 entries were displayed.
```

   O exemplo a seguir mostra a cota de árvore para o volume FlexGroup FG1:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
fg1      qtree1  tree      1         68KB      -      18       -
qtree1
fg1              tree      *           0B      -       0       -   *
2 entries were displayed.
```

Resultados

As regras e limites de quota são aplicados no volume FlexGroups.

O uso pode chegar até 5% mais alto do que um limite rígido configurado antes que o ONTAP força a cota rejeitando mais tráfego.

Informações relacionadas

- "Referência do comando ONTAP"

Habilite a eficiência de storage em um volume FlexGroup

Você pode executar deduplicação e compactação de dados em conjunto ou de forma independente em um volume FlexGroup para obter a melhor economia de espaço.

O que você vai precisar

O volume FlexGroup deve estar online.

Passos

1. Habilite a eficiência de storage no volume FlexGroup: `volume efficiency on -vserver svm_name -volume volume_name`

   As operações de eficiência de storage são ativadas em todos os componentes do volume FlexGroup.

   Se um volume de FlexGroup for expandido depois que a eficiência de storage for habilitada no volume, a eficiência de storage será automaticamente ativada nos novos componentes.

2. Ative a operação de eficiência de storage necessária no volume FlexGroup usando o `volume efficiency modify` comando.

   Você pode habilitar a deduplicação in-line, a deduplicação pós-processo, a compactação in-line e a compactação pós-processo em volumes FlexGroup. Você também pode definir o tipo de compactação (secundária ou adaptável) e especificar uma programação ou política de eficiência para o volume FlexGroup.

3. Se você não estiver usando programações ou políticas de eficiência para executar as operações de eficiência de storage, inicie a operação de eficiência: `volume efficiency start -vserver svm_name -volume volume_name`

   Se a deduplicação e a compactação de dados estiverem habilitadas em um volume, a compactação de dados será executada inicialmente seguida pela deduplicação. Este comando falha se alguma operação de eficiência já estiver ativa no volume FlexGroup.

4. Verifique as operações de eficiência ativadas no volume FlexGroup: `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
             Vserver Name: vs1
              Volume Name: fg1
              Volume Path: /vol/fg1
                    State: Enabled
                   Status: Idle
                 Progress: Idle for 17:07:25
                     Type: Regular
                 Schedule: sun-sat@0

...

              Compression: true
      Inline Compression: true
Incompressible Data Detection: false
      Constituent Volume: false
Compression Quick Check File Size: 524288000
           Inline Dedupe: true
         Data Compaction: false
```

Proteja volumes FlexGroup com cópias Snapshot

Você pode criar políticas do Snapshot que gerenciam automaticamente a criação de cópias Snapshot ou podem criar cópias Snapshot manualmente para volumes do FlexGroup. Uma cópia Snapshot válida é criada para um volume FlexGroup somente depois que o ONTAP puder criar com êxito uma cópia Snapshot para cada componente do volume FlexGroup.

Sobre esta tarefa

- Se você tiver vários volumes do FlexGroup associados a uma política Snapshot, verifique se as programações do FlexGroup volumes não se sobrepõem.
- A partir do ONTAP 9.8, o número máximo de cópias snapshot com suporte para um volume FlexGroup é de 1023.

> ⓘ A partir do ONTAP 9.8, o `volume snapshot show` comando do FlexGroup volumes relata o tamanho da cópia Snapshot usando blocos lógicos, em vez de calcular os blocos de propriedade mais novos. Esse novo método de cálculo de tamanho pode fazer com que o tamanho da cópia Snapshot pareça maior do que os cálculos em versões anteriores do ONTAP.

Passos

1. Criar uma política de snapshot ou criar manualmente uma cópia Snapshot:

Se você quiser criar um…	Digite este comando…

Política do Snapshot	`volume snapshot policy create` As programações associadas à política de snapshot de um volume FlexGroup devem ter um intervalo maior que 30 minutos. Quando você cria um volume FlexGroup, a `default` política Snapshot é aplicada ao volume FlexGroup.
Cópia Snapshot manualmente	`volume snapshot create` Depois de criar uma cópia Snapshot para um volume FlexGroup, não é possível modificar os atributos da cópia Snapshot. Se você quiser modificar os atributos, exclua e crie novamente a cópia Snapshot.

O acesso do cliente ao volume FlexGroup é rapidamente interrompido quando uma cópia Snapshot é criada.

1. Verifique se foi criada uma cópia Snapshot válida para o volume FlexGroup: `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
------- ------ ---------------------- -----
fg_vs   fg     hourly.2016-08-23_0505 valid
```

2. Veja as cópias Snapshot dos componentes do volume FlexGroup: `volume snapshot show -is -constituent true`

```
cluster1::> volume snapshot show -is-constituent true

---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
fg_vs    fg__0001
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0002
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0003
                  hourly.2016-08-23_0505                    72MB     0%
27%
...
         fg__0016
                  hourly.2016-08-23_0505                    72MB     0%
27%
```

Mova os componentes de um volume FlexGroup

Você pode mover os constituintes de um volume FlexGroup de um agregado para outro para equilibrar a carga quando certos constituintes experimentam mais tráfego. Mover constituintes também ajuda a liberar espaço em um agregado para redimensionar os constituintes existentes.

O que você vai precisar

Para mover um componente de volume FlexGroup que está em uma relação SnapMirror, você deve ter inicializado a relação SnapMirror.

Sobre esta tarefa

Não é possível executar uma operação de movimentação de volume enquanto os constituintes do volume FlexGroup estão sendo expandidos.

Passos

1. Identifique o componente de volume FlexGroup que você deseja mover:

   ```
   volume show -vserver svm_name -is-constituent true
   ```

```
cluster1::> volume show -vserver vs2 -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2       fg1          -            online     RW        400TB
15.12TB   62%
vs2       fg1__0001    aggr1        online     RW         25TB
8.12MB   59%
vs2       fg1__0002    aggr2        online     RW         25TB
2.50TB   90%
...
```

2. Identifique um agregado para o qual você pode mover o componente de volume FlexGroup:

   `volume move target-aggr show -vserver svm_name -volume vol_constituent_name`

   O espaço disponível no agregado que você selecionar deve ser maior que o tamanho do componente de volume FlexGroup que você está movendo.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9TB          hdd
node12a_aggr3    100.34TB         hdd
node12a_aggr2    100.36TB         hdd
node12a_aggr1    100.36TB         hdd
node12a_aggr4    100.36TB         hdd
5 entries were displayed.
```

3. Verifique se o componente de volume FlexGroup pode ser movido para o agregado pretendido:

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name -perform-validation-only true`

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

4. Mova o componente de volume FlexGroup:

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name [-allow-mixed-aggr-types {true|false}]`

   A operação de movimentação de volume é executada como um processo em segundo plano.

A partir do ONTAP 9.5, é possível mover os componentes de volume FlexGroup de um pool de malha para um pool que não seja de malha ou vice-versa definindo o `-allow-mixed-aggr-types` parâmetro para `true`. Por padrão, a `-allow-mixed-aggr-types` opção é definida como `false`.

> Não é possível usar o `volume move` comando para ativar a criptografia em volumes FlexGroup.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```

> Se a operação de movimentação de volume falhar devido a uma operação SnapMirror ativa, você deve cancelar a operação SnapMirror usando o `snapmirror abort -h` comando. Em alguns casos, a operação de cancelamento do SnapMirror também pode falhar. Em tais situações, você deve cancelar a operação de movimentação de volume e tentar novamente mais tarde.

5. Verifique o estado da operação de movimentação de volume:

   `volume move show -volume vol_constituent_name`

   O exemplo a seguir mostra o estado de um volume constituinte do FlexGroup que concluiu a fase de replicação e está na fase de transição da operação de movimentação de volume:

```
cluster1::> volume move show -volume fg1_002
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       fg1_002    healthy  cutover     -                -
```

Usar agregados no FabricPool para volumes FlexGroup existentes

A partir do ONTAP 9.5, o FabricPool é compatível com volumes FlexGroup. Se você quiser usar agregados no FabricPool para seus volumes FlexGroup existentes, você pode converter os agregados nos quais o volume FlexGroup reside em agregados no FabricPool ou migrar os componentes de volume FlexGroup para agregados no FabricPool.

O que você vai precisar

- O volume FlexGroup deve ter garantia de espaço definida como `none`.
- Para converter os agregados nos quais o volume FlexGroup reside em agregados no FabricPool, os agregados devem estar usando todos os discos SSD.

Sobre esta tarefa

Se um volume FlexGroup existente residir em agregados que não sejam SSD, é necessário migrar os componentes de volume FlexGroup para agregados no FabricPool.

Opções

- Para converter os agregados nos quais o volume FlexGroup reside em agregados no FabricPool, execute as seguintes etapas:

  a. Defina a política de disposição em categorias no volume FlexGroup existente: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. Identificar os agregados nos quais reside o volume FlexGroup: `volume show -volume flexgroup_name -fields aggr-list`

  ```
  cluster-2::> volume show -volume fg1 -fields aggr-list
  vserver volume aggr-list
  ------- ------ -----------
  vs1     fg1    aggr1,aggr3
  ```

  c. Anexe um armazenamento de objetos a cada agregado listado na lista de agregados: `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

  É necessário anexar todos os agregados a um armazenamento de objetos.

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- Para migrar os componentes de volume FlexGroup para agregados no FabricPool, execute as seguintes etapas:

  a. Defina a política de disposição em categorias no volume FlexGroup existente: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. Mova cada componente do volume FlexGroup para um agregado no FabricPool no mesmo cluster: `volume move start -volume constituent-volume -destination-aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

  É necessário mover todos os componentes de volume FlexGroup para agregados no FabricPool (caso os componentes de volume FlexGroup estejam em tipos de agregados mistos) e garantir que todos os componentes estejam balanceados nos nós do cluster.

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

Informações relacionadas

"Gerenciamento de disco e agregado"

Equilibre os volumes do ONTAP FlexGroup redistribuindo dados de arquivos

A partir do ONTAP 9.16,1, é possível habilitar o balanceamento avançado de capacidade para permitir a distribuição de dados entre os volumes membros do FlexGroup quando arquivos muito grandes crescem e consomem espaço em um volume de membro.

O balanceamento avançado de capacidade expande a funcionalidade de dados granulares introduzida no ONTAP 9.12,1, que permite ao ONTAP "Rebalancear os volumes FlexGroup"mover arquivos para outros membros. A partir do ONTAP 9.16,1, quando o balanceamento avançado de capacidade é ativado com a `-granular-data advanced` opção, os recursos de rebalanceamento de arquivos "básicos", bem como os recursos avançados de capacidade são ativados.

> O rebalanceamento de arquivos e o balanceamento avançado de capacidade são desativados por padrão. Depois que esses recursos estiverem ativados, eles não poderão ser desativados. Se você precisar desativar o balanceamento de capacidade, será necessário restaurar a partir de um snapshot criado antes que o balanceamento avançado de capacidade tenha sido habilitado.

O balanceamento avançado de capacidade é acionado por novas gravações chegando a 10GB ou 1% do espaço livre de um volume.

Como os arquivos são distribuídos

Se um arquivo for criado ou for grande o suficiente para acionar o balanceamento de capacidade avançado, o arquivo será distribuído em faixas entre 1GB e 10GB nos volumes FlexGroup membros.

Quando o balanceamento avançado de capacidade estiver ativado, o ONTAP não fará o particionamento retroativo de arquivos grandes existentes. Se um arquivo grande existente continuar a crescer depois que o balanceamento avançado de capacidade estiver habilitado, o novo conteúdo em arquivos grandes existentes pode ser distribuído entre os volumes FlexGroup membros, dependendo do tamanho do arquivo e do espaço disponível.

O balanceamento de capacidade avançado determina a largura da faixa é usando a quantidade de espaço livre disponível no volume do membro. O balanceamento avançado de capacidade cria uma distribuição de arquivos que representa 1% do espaço livre disponível. Isso significa que as listras podem começar maiores se houver mais espaço disponível, e elas se tornam menores à medida que o FlexGroup se enche.

Além do espaço disponível no volume do membro, o balanceamento avançado de capacidade usa vários outros fatores para determinar a largura da faixa:

- Largura mínima da faixa: A menor largura de faixa já escolhida é 1GBmm.
- Largura máxima da faixa: A maior largura possível da faixa é de 10GBmm.
- Granularidade: As listras são sempre criadas em múltiplos de 1GB.

Protocolos compatíveis

O balanceamento avançado de capacidade é compatível com os seguintes protocolos:

- NFSv3, NFSv4, NFSv4.1

- PNFS
- SMB

Ative o balanceamento de capacidade avançado

O balanceamento avançado de capacidade está desativado por padrão. Você deve habilitar o balanceamento avançado de capacidade para equilibrar automaticamente a capacidade do FlexGroup. Tenha em mente que não é possível desativar esse recurso depois de ativá-lo, mas você pode restaurar a partir de um snapshot criado antes que o balanceamento avançado de capacidade tenha sido ativado.

Antes de começar

- Todos os nós no cluster devem estar executando o ONTAP 9.16,1 ou posterior.
- Não é possível reverter para uma versão anterior ao ONTAP 9.16,1 se o balanceamento avançado de capacidade estiver ativado. Se você precisar reverter, primeiro será necessário restaurar a partir de um snapshot criado antes que o balanceamento avançado de capacidade tenha sido habilitado.
- Se a descarga de cópia NFS tiver sido ativada (`vserver nfs -vstorage enabled`) em uma SVM, você não poderá ativar o balanceamento avançado de capacidade em um volume FlexGroup. Da mesma forma, se o balanceamento avançado de capacidade estiver habilitado em qualquer volume FlexGroup em uma SVM, não será possível ativar a descarga de cópia NFS.
- O balanceamento avançado de capacidade não é compatível com o FlexCache writeback.
- As transferências SnapMirror não são compatíveis com versões do ONTAP anteriores ao ONTAP 9.16.1 quando o balanceamento avançado de capacidade está habilitado em volumes em clusters que executam o ONTAP 9.16.1 ou posterior.

Sobre esta tarefa

Durante a criação de volumes de destino DP usando uma das opções de dados granulares (básico ou avançado), o destino exibe a configuração como "desativado" até que a transferência SnapMirror seja concluída. Após a conclusão da transferência, o destino DP exibe dados granulares como "ativado".

Ative o balanceamento de capacidade avançado durante a criação do FlexGroup

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para habilitar o balanceamento avançado de capacidade ao criar um novo volume FlexGroup.

System Manager

1. Navegue até **Storage > volumes** e clique  em .
2. Na janela **Adicionar volume**, insira o nome e o tamanho do volume. Em seguida, clique em **mais opções**.
3. Em **armazenamento e otimização**, selecione **distribuir dados de volume pelo cluster (FlexGroup)**.
4. Selecione **balanceamento de capacidade avançado**.
5. Termine de configurar o volume e clique em **Save**.

CLI

1. Crie um volume com o balanceamento de capacidade avançado ativado:

```
volume create -vserver <svm name> -volume <volume name>-size <volume
size> -auto-provision-as flexgroup -junction-path /<path> -granular
-data advanced
```

Exemplo:

```
volume create -vserver vs0 -volume newvol-size 1TB -auto-provision
-as flexgroup -junction-path /newvol -granular-data advanced
```

Habilite o balanceamento de capacidade avançado em volumes FlexGroup existentes

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para habilitar o balanceamento avançado de capacidade.

System Manager

1. Navegue até **armazenamento > volumes**, clique ⋮ em e escolha **Editar > volume**.
2. Na janela **Editar volume**, em **armazenamento e otimização**, selecione **balanceamento avançado de capacidade**.
3. Clique em **Salvar**.

CLI

1. Modifique um volume FlexGroup existente para habilitar o balanceamento avançado de capacidade:

```
volume modify -vserver <svm name> -volume <volume name> -granular
-data advanced
```

Exemplo:

```
volume modify -vserver vs0 -volume newvol  -granular-data advanced
```

Rebalanceie volumes do FlexGroup com a movimentação de arquivos

A partir do ONTAP 9.12,1, você pode rebalancear volumes FlexGroup movendo arquivos de um componente em um FlexGroup para outro componente sem interrupções.

O rebalanceamento do FlexGroup ajuda a redistribuir a capacidade quando os desequilíbrios se desenvolvem ao longo do tempo devido à adição de novos arquivos e ao crescimento de arquivos. Depois de iniciar manualmente a operação de rebalancear, o ONTAP seleciona os arquivos e os move automaticamente e sem interrupções.

> ⓘ Você deve estar ciente de que o rebalanceamento do FlexGroup degrada o desempenho do sistema quando um grande número de arquivos é movido como parte de um único evento de rebalanceamento ou sobre vários eventos de rebalanceamento devido à criação de inodes de várias partes. Cada arquivo movido como parte de um evento de rebalanceamento tem 2 inodes de várias partes associadas a esse arquivo. Quanto maior o número de arquivos com inodes multipartes como uma porcentagem do número total de arquivos em um FlexGroup, maior o impactos no desempenho. Certos casos de uso, como uma conversão de FlexVol para FlexGroup, podem resultar em uma quantidade significativa de criação de inodes em várias partes.

O rebalanceamento está disponível somente quando todos os nós do cluster estiverem executando o ONTAP 9.12,1 ou versões posteriores. Você deve habilitar a funcionalidade de dados granulares em qualquer volume do FlexGroup que execute a operação de rebalanceamento. Depois que essa funcionalidade estiver ativada, você não poderá reverter para o ONTAP 9.11,1 e versões anteriores, a menos que você exclua esse volume ou restauração de uma cópia Snapshot criada antes que a configuração fosse ativada.

A partir do ONTAP 9.14,1, o ONTAP apresenta um algoritmo para mover arquivos em volumes com dados granulares ativados sem interação do usuário, sem interrupções e proativamente. O algoritmo opera em cenários muito específicos e direcionados para aliviar gargalos de desempenho. Os cenários em que esse algoritmo pode agir incluem carga de gravação muito pesada em um conjunto específico de arquivos em um

nó no cluster ou um arquivo em crescimento contínuo em um diretório pai muito quente.

A partir do ONTAP 9.16,1, você também pode habilitar "balanceamento de capacidade avançado"a redistribuir dados de um arquivo grande entre os volumes membros do FlexGroup.

Considerações sobre o rebalanceamento do FlexGroup

Você deve estar ciente de como o rebalanceamento do FlexGroup funciona e como ele interage com outros recursos do ONTAP.

- Conversão de FlexVol para FlexGroup

  É recomendável que você *não* use o rebalanceamento automático do FlexGroup após uma conversão de FlexVol para FlexGroup. Em vez disso, você pode usar o recurso de movimentação de arquivos retroativos disruptivos disponível no ONTAP 9.10,1 e posterior, digitando o `volume rebalance file-move` comando. Para obter a sintaxe de comando, consulte a `volume rebalance file-move start` página man.

  O rebalanceamento com o recurso de rebalanceamento automático do FlexGroup pode degradar o desempenho ao mover um grande número de arquivos, como quando você executa uma conversão de FlexVol para FlexGroup, e até 50 a 85% dos dados no FlexVol volume são movidos para um novo componente.

- Tamanho mínimo e máximo do arquivo

  A seleção de arquivos para rebalanceamento automático é baseada em blocos salvos. O tamanho mínimo de arquivo considerado para rebalanceamento é de 100 MB por padrão (pode ser configurado tão baixo quanto 20 MB usando o parâmetro min-file-size mostrado abaixo) e o tamanho máximo do arquivo é de 100 GB.

- Arquivos nas cópias Snapshot

  Você pode configurar o rebalanceamento do FlexGroup para considerar apenas os arquivos a serem movidos que não estão presentes atualmente em nenhuma cópia Snapshot. Quando o rebalanceamento é iniciado, uma notificação é exibida se uma operação de cópia Snapshot for agendada a qualquer momento durante uma operação de rebalanceamento.

  As cópias snapshot ficam restritas se um arquivo estiver sendo movido e estiver passando por enquadramento no destino. Uma operação de restauração de cópia Snapshot não é permitida enquanto o rebalanceamento de arquivos estiver em andamento.

  Qualquer cópia Snapshot criada após a `granular-data` opção ser ativada não pode ser replicada para um sistema que executa o ONTAP 9.11,1 e versões anteriores porque o ONTAP 9.11,1 e versões anteriores não suportam inodes de várias partes.

- Operações da SnapMirror

  O rebalanceamento do FlexGroup deve ocorrer entre operações SnapMirror agendadas. Uma operação SnapMirror pode falhar se um arquivo estiver sendo relocado antes que uma operação SnapMirror comece se essa movimentação de arquivo não for concluída dentro do período de 24 minutos de tentativa do SnapMirror. Qualquer nova realocação de arquivo que comece após uma transferência do SnapMirror ser iniciada não falhará.

- Eficiência de storage de compressão baseada em arquivo

Com a eficiência de storage de compactação baseado em arquivo, o arquivo é descompactado antes de ser movido para o destino. Assim, a economia de compactação será perdida. A economia de compressão é recuperada depois que um scanner de fundo iniciado manualmente é executado no volume FlexGroup após o rebalanceamento. No entanto, se qualquer arquivo estiver associado a uma cópia Snapshot em qualquer volume, o arquivo será ignorado para compactação.

- Deduplicação

  Mover arquivos desduplicados pode causar maior uso geral do volume FlexGroup. Durante o rebalanceamento de arquivos, apenas blocos exclusivos são movidos para o destino, liberando essa capacidade na origem. Os blocos compartilhados permanecem na origem e são copiados para o destino. Embora isso alcance o objetivo de reduzir a capacidade usada em um componente de origem quase completa, ele também pode levar ao aumento do uso geral no volume FlexGroup devido a cópias de blocos compartilhados nos novos destinos. Isso também é possível quando os arquivos que fazem parte de uma cópia Snapshot são movidos. A economia de espaço não será totalmente reconhecida até que o agendamento de cópia Snapshot seja reciclado e não haja mais cópias dos arquivos nas cópias Snapshot.

- Volumes FlexClone

  Se o rebalanceamento de arquivos estiver em andamento quando um volume FlexClone for criado, o rebalanceamento não será realizado no volume FlexClone. O rebalanceamento no volume FlexClone deve ser realizado após a criação.

- Movimentação de arquivos

  Quando um arquivo é movido durante uma operação de rebalanceamento do FlexGroup, o tamanho do arquivo é relatado como parte da contagem de cotas nos componentes de origem e destino. Quando a movimentação estiver concluída, a contagem de cotas retorna ao normal e o tamanho do arquivo só é relatado no novo destino.

- Proteção autônoma contra ransomware

  A partir do ONTAP 9.13,1, a proteção autônoma contra ransomware é suportada durante operações de rebalanceamento ininterruptas e sem interrupções.

- Volumes de armazenamento de objetos

  O rebalanceamento da capacidade de volume não é compatível com volumes de armazenamento de objetos, como buckets do S3.

Ative o rebalanceamento do FlexGroup

A partir do ONTAP 9.12,1, é possível habilitar o rebalanceamento automático de volume FlexGroup sem interrupções para redistribuir arquivos entre componentes do FlexGroup.

A partir do ONTAP 9.13,1, você pode agendar uma única operação de rebalanceamento do FlexGroup para começar em uma data e hora no futuro.

Antes de começar

Você deve ter habilitado a `granular-data` opção no volume FlexGroup antes de ativar o rebalanceamento do FlexGroup. Você pode ativá-lo usando um destes métodos:

- Quando você cria o volume FlexGroup usando o `volume create` comando
- Modificando um volume FlexGroup existente para ativar a configuração usando o `volume modify`

comando

- Definindo-o automaticamente quando o rebalanceamento do FlexGroup é iniciado usando o `volume rebalance` comando

> Se você estiver usando o ONTAP 9.16,1 ou posterior e "Balanceamento de capacidade avançado do FlexGroup" estiver habilitado usando a `granular-data advanced` opção na CLI do ONTAP ou usando o Gerenciador de sistema, o rebalanceamento do FlexGroup também será ativado.

Passos

Você pode gerenciar o rebalanceamento do FlexGroup usando o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

System Manager

1. Navegue até **armazenamento > volumes** e localize o volume FlexGroup para reequilibrar.
2. Selecione para ver os detalhes do volume.
3. Em **Estado do saldo do FlexGroup** selecione **Rebalancamento**.

   A opção **Rebalancamento** só está disponível quando o status FlexGroup estiver fora de equilíbrio.

4. Na janela **Rebalancar volume**, altere as configurações padrão conforme necessário.
5. Para agendar a operação de rebalanceamento, selecione **reequilibrar mais tarde** e insira a data e a hora.

CLI

1. Iniciar o reequilíbrio automático:

   ```
   volume rebalance start -vserver <SVM name> -volume <volume name>
   ```

   Opcionalmente, você pode especificar as seguintes opções:

   [[-Max-runtime] <time interval>] tempo de execução máximo

   [-Max-threshold <percent>] limite máximo de desequilíbrio por constituinte

   [-min-threshold <percent>] limiar mínimo de desequilíbrio por constituinte

   [-max-file-moves <integer>] o máximo de movimentos simultâneos de arquivos por constituinte

   Tamanho mínimo do ficheiro [<integer>[KB|MB|GB|TB|PB]]]

   [-start-time <mm/dd/yyyy-00:00:00>] Agendar rebalanceamento data e hora de início

   [-exclude-snapshots] excluem arquivos presos em cópias Snapshot

   Exemplo:

   ```
   volume rebalance start -vserver vs0 -volume fg1
   ```

Modificar as configurações de rebalancear do FlexGroup

Você pode alterar uma configuração de rebalanceamento do FlexGroup para atualizar o limite de desequilíbrio, o número de arquivos simultâneos move o tamanho mínimo do arquivo, o tempo de execução máximo e para incluir ou excluir cópias Snapshot. As opções para modificar seu cronograma de rebalanceamento do FlexGroup estão disponíveis a partir do ONTAP 9.13,1.

System Manager

1. Navegue até **armazenamento > volumes** e localize o volume FlexGroup para reequilibrar.
2. Selecione para ver os detalhes do volume.
3. Em **Estado do saldo do FlexGroup** selecione **Rebalancamento**.

   A opção **Rebalancamento** só está disponível quando o status FlexGroup estiver fora de equilíbrio.

4. Na janela **Rebalancar volume**, altere as configurações padrão conforme necessário.

CLI

1. Modificar o reequilíbrio automático:

   ```
   volume rebalance modify -vserver <SVM name> -volume <volume name>
   ```

   Pode especificar uma ou mais das seguintes opções:

   [[-Max-runtime] <time interval>] tempo de execução máximo

   [-Max-threshold <percent>] limite máximo de desequilíbrio por constituinte

   [-min-threshold <percent>] limiar mínimo de desequilíbrio por constituinte

   [-max-file-moves <integer>] o máximo de movimentos simultâneos de arquivos por constituinte

   Tamanho mínimo do ficheiro [<integer>[KB|MB|GB|TB|PB]]]

   [-start-time <mm/dd/yyyy-00:00:00>] Agendar rebalanceamento data e hora de início

   [-exclude-snapshots] excluem arquivos presos em cópias Snapshot

Parar o rebalancear FlexGroup

Depois que o rebalanceamento do FlexGroup estiver ativado ou programado, você poderá pará-lo a qualquer momento.

System Manager

1. Navegue até **armazenamento > volumes** e localize o volume FlexGroup.
2. Selecione para ver os detalhes do volume.
3. Selecione **Parar reequilíbrio**.

CLI

1. Parar o reequilíbrio do FlexGroup:

```
volume rebalance stop -vserver <SVM name> -volume <volume name>
```

Visualizar o status do FlexGroup Rebalanceance

Você pode exibir o status de uma operação de rebalancear a FlexGroup, a configuração do FlexGroup Rebalancamento, o tempo de operação no rebalancear e os detalhes da instância.

System Manager

1. Navegue até **armazenamento > volumes** e localize o volume FlexGroup.
2. Selecione para ver os detalhes do FlexGroup.
3. **Status do saldo do FlexGroup** é exibido perto da parte inferior do painel de detalhes.
4. Para ver informações sobre a última operação de reequilíbrio, selecione **Estado de reequilíbrio do último volume**.

CLI

1. Veja o status de uma operação de rebalanceamento do FlexGroup:

```
volume rebalance show
```

Exemplo de estado de rebalanceamento:

```
> volume rebalance show
Vserver: vs0
                                                                  Target
Imbalance
Volume       State                  Total      Used     Used
Size     %
------------ ------------------ --------- --------- ---------
--------- -----
fg1          idle                     4GB   115.3MB         -
8KB    0%
```

Exemplo de detalhes de configuração do rebalanceamento:

```
> volume rebalance show -config
Vserver: vs0
                     Max            Threshold         Max
Min          Exclude
Volume               Runtime        Min     Max       File Moves
File Size    Snapshot
---------------      ------------   -----   -----     ----------
---------    ---------
fg1                  6h0m0s         5%      20%          25
4KB          true
```

Exemplo de detalhes do tempo de rebalanceamento:

```
> volume rebalance show -time
Vserver: vs0
Volume               Start Time                    Runtime
Max Runtime
---------------     -------------------------     -----------
-----------
fg1                  Wed Jul 20 16:06:11 2022      0h1m16s
6h0m0s
```

Exemplo de detalhes da instância de rebalancear:

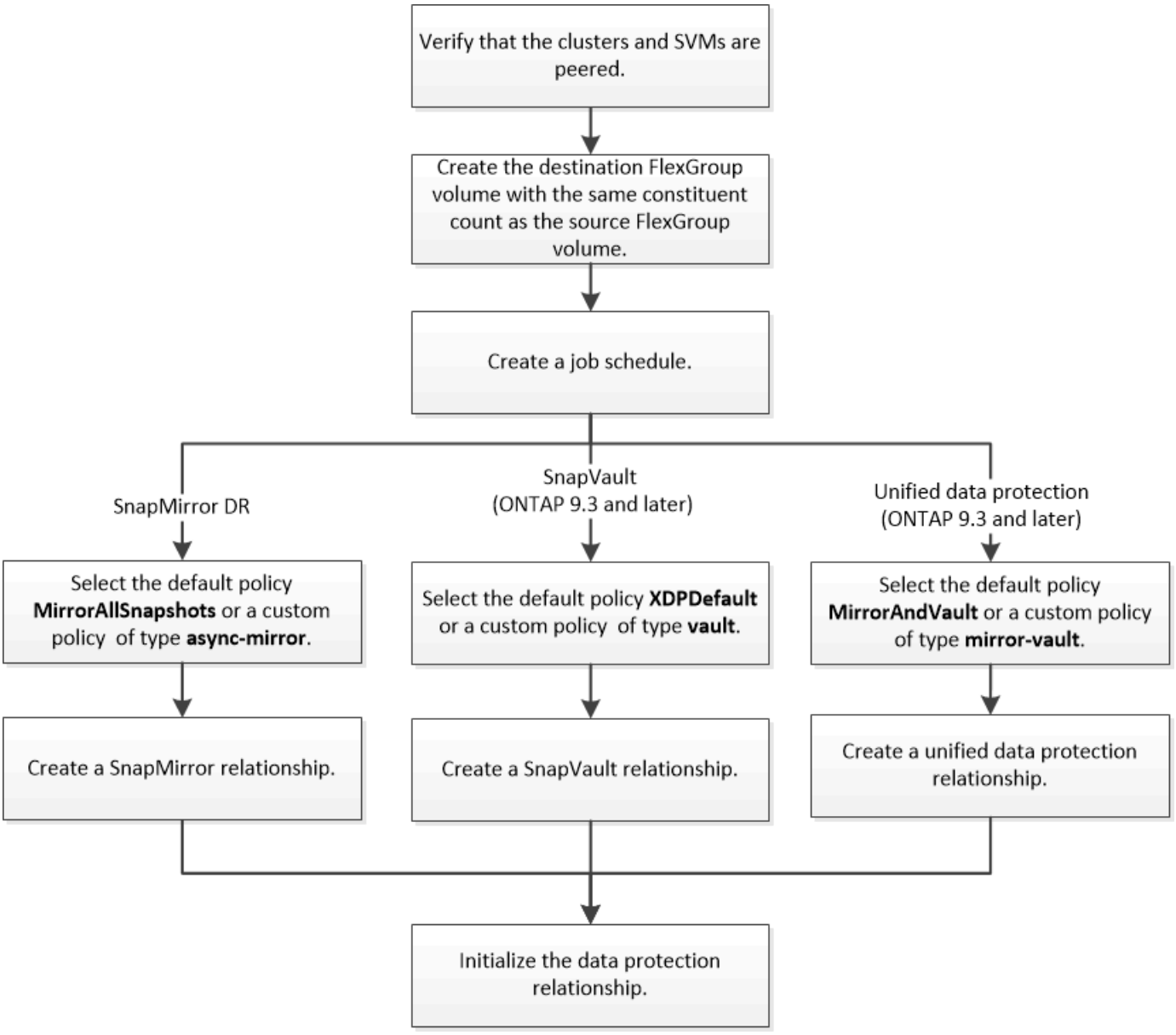
```
> volume rebalance show -instance
Vserver Name: vs0
Volume Name: fg1
Is Constituent: false
Rebalance State: idle
Rebalance Notice Messages: -
Total Size: 4GB
AFS Used Size: 115.3MB
Constituent Target Used Size: -
Imbalance Size: 8KB
Imbalance Percentage: 0%
Moved Data Size: -
Maximum Constituent Imbalance Percentage: 1%
Rebalance Start Time: Wed Jul 20 16:06:11 2022
Rebalance Stop Time: -
Rebalance Runtime: 0h1m32s
Rebalance Maximum Runtime: 6h0m0s
Maximum Imbalance Threshold per Constituent: 20%
Minimum Imbalance Threshold per Constituent: 5%
Maximum Concurrent File Moves per Constituent: 25
Minimum File Size: 4KB
Exclude Files Stuck in Snapshot Copies: true
```

Proteção de dados para FlexGroup volumes

Fluxo de trabalho de proteção de dados para FlexGroup volumes

Você pode criar relacionamentos de recuperação de desastres (DR) do SnapMirror para o FlexGroup volumes. A partir do ONTAP 9.3, você também pode fazer backup e restaurar volumes do FlexGroup com a tecnologia SnapVault. Além disso, você pode criar um relacionamento de proteção de dados unificado que usa o mesmo destino para backup e recuperação de desastres.

O fluxo de trabalho de proteção de dados consiste em verificar os relacionamentos entre cluster e colegas SVM, criar um volume de destino, criar um cronograma de trabalho, especificar uma política, criar um relacionamento de proteção de dados e inicializar o relacionamento.



Sobre esta tarefa

O tipo de relação do SnapMirror é sempre `XDP` para volumes do FlexGroup. O tipo de proteção de dados fornecido por um relacionamento do SnapMirror é determinado pela política de replicação que você usa. Você pode usar a política padrão ou uma política personalizada do tipo necessário para o relacionamento de replicação que deseja criar. A tabela a seguir mostra os tipos de política padrão e os tipos de política personalizada compatíveis para diferentes tipos de relacionamentos de proteção de dados.

Tipo de relação	Política padrão	Tipo de política personalizada
SnapMirror DR	MirrorAllinstantâneos	espelho assíncrono
Backup SnapVault	XDPDefat	cofre

Proteção de dados unificada	MirrorAndVault	espelho-cofre

A política MirrorLatest não é suportada com volumes FlexGroup.

Criar uma relação do SnapMirror para o FlexGroup volumes

Você pode criar uma relação de SnapMirror entre o volume FlexGroup de origem e o volume FlexGroup de destino em uma SVM com peered para replicação de dados para recuperação de desastres. Você pode usar as cópias espelhadas do volume FlexGroup para recuperar dados quando ocorre um desastre.

Antes de começar

Você precisa ter criado a relação de peering de cluster e a relação de peering SVM.

"Peering de cluster e SVM"

Sobre esta tarefa

- A partir do ONTAP 9,9.1, você pode usar a CLI do ONTAP para criar relações em cascata e fanout do SnapMirror para volumes do FlexGroup. Para obter detalhes, "Considerações para criar relações de cascata e fanout do SnapMirror para FlexGroups"consulte .
- Você pode criar relacionamentos SnapMirror entre clusters e relacionamentos SnapMirror entre clusters para volumes FlexGroup.
- A partir do ONTAP 9.3, é possível expandir volumes do FlexGroup que estão em uma relação do SnapMirror.

  Se você estiver usando uma versão do ONTAP anterior à ONTAP 9.3, não será necessário expandir os volumes do FlexGroup depois que um relacionamento do SnapMirror for estabelecido. No entanto, você poderá aumentar a capacidade dos volumes do FlexGroup após estabelecer um relacionamento do SnapMirror. Se você expandir o volume FlexGroup de origem depois de quebrar a relação SnapMirror em versões anteriores ao ONTAP 9.3, será necessário realizar uma transferência de linha de base para o volume FlexGroup de destino.

Passos

1. Crie um volume FlexGroup de destino do tipo `DP` que tenha o mesmo número de constituintes do volume FlexGroup de origem:
   a. A partir do cluster de origem, determine o número de componentes no volume FlexGroup de origem: `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. A partir do cluster de destino, crie um volume do tipo FlexGroup de destino `DP` com o mesmo número de componentes que o do volume FlexGroup de origem.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. A partir do cluster de destino, verifique o número de componentes no volume FlexGroup de destino: `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume        Aggregate    State      Type       Size
Available  Used%
--------- ------------  ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     DP         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     DP         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     DP         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     DP         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     DP         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     DP         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     DP         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     DP         25TB
10.63TB   57%
...
```

2. Criar uma agenda de trabalhos: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para as `-month` opções , `-dayofweek`, e `-hour` , é possível especificar `all` para executar o trabalho todos os meses, todos os dias da semana e a cada hora, respetivamente.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. Crie uma política de tipo personalizada `async-mirror` para o relacionamento SnapMirror: `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

   Se você não criar uma política personalizada, especifique a `MirrorAllSnapshots` política para relacionamentos do SnapMirror.

4. No cluster de destino, crie uma relação SnapMirror entre o volume FlexGroup de origem e o volume FlexGroup de destino: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

As relações do SnapMirror para volumes do FlexGroup devem ser do tipo `XDP`.

Se você especificar um valor do acelerador para a relação SnapMirror para o volume FlexGroup, cada componente usará o mesmo valor do acelerador. O valor da borboleta não está dividido entre os componentes.

Não é possível usar rótulos SnapMirror de cópias Snapshot para volumes FlexGroup.

No ONTAP 9.4 e anteriores, se a política não for especificada com o `snapmirror create` comando, a `MirrorAllSnapshots` política será usada por padrão. No ONTAP 9.5, se a política não for especificada com o `snapmirror create` comando, a `MirrorAndVault` política será usada por padrão.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly
Operation succeeded: snapmirror create for the relationship with
destination "vsd:dstFG".
```

5. A partir do cluster de destino, inicialize a relação SnapMirror executando uma transferência de linha de base: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   Após a conclusão da transferência da linha de base, o volume FlexGroup de destino é atualizado periodicamente com base na programação da relação SnapMirror.

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

Se você tiver criado qualquer relação do SnapMirror entre o FlexGroup volumes com o cluster de origem que executa o ONTAP 9.3 e o cluster de destino que executa o ONTAP 9.2 ou anterior, e se você criar qtrees no volume FlexGroup de origem, as atualizações do SnapMirror falharão. Para se recuperar dessa situação, você deve excluir todos os qtrees não-padrão no volume FlexGroup, desativar a funcionalidade de qtree no volume FlexGroup e excluir todas as cópias Snapshot que estão habilitadas com a funcionalidade de qtree.

Depois de terminar

Você deve configurar o SVM de destino para acesso aos dados configurando as configurações necessárias, como LIFs e políticas de exportação.

Criar uma relação do SnapVault para o FlexGroup volumes

Você pode configurar uma relação do SnapVault e atribuir uma política do SnapVault à relação para criar um backup do SnapVault.

O que você vai precisar

Você precisa estar ciente das considerações para criar uma relação do SnapVault para o FlexGroup volumes.

Passos

1. Crie um volume FlexGroup de destino do tipo `DP` que tenha o mesmo número de constituintes do volume

FlexGroup de origem:

a. A partir do cluster de origem, determine o número de componentes no volume FlexGroup de origem:
`volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume src* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       src          -            online     RW         400TB
172.86GB  56%
vss       src__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       src__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       src__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       src__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       src__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       src__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       src__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. A partir do cluster de destino, crie um volume do tipo FlexGroup de destino `DP` com o mesmo número de componentes que o do volume FlexGroup de origem.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst

Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. A partir do cluster de destino, verifique o número de componentes no volume FlexGroup de destino:
`volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dst* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     RW         400TB
172.86GB  56%
vsd       dst__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dst__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dst__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dst__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dst__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dst__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dst__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. Criar uma agenda de trabalhos: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Crie uma política SnapVault e defina uma regra para a política SnapVault:

   a. Crie uma política de tipo personalizada `vault` para o relacionamento SnapVault: `snapmirror policy create -vserver svm_name -policy policy_name -type vault`

   b. Defina uma regra para a política do SnapVault que determina quais cópias snapshot serão transferidas durante as operações de inicialização e atualização: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   Se você não criar uma política personalizada, especifique a `XDPDefault` política para relacionamentos do SnapVault.

4. Criar uma relação SnapVault: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

   No ONTAP 9.4 e anteriores, se a política não for especificada com o `snapmirror create` comando, a `MirrorAllSnapshots` política será usada por padrão. No ONTAP 9.5, se a política não for especificada com o `snapmirror create` comando, a `MirrorAndVault` política será usada por padrão.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

5. A partir do cluster de destino, inicialize a relação SnapVault executando uma transferência de linha de base: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

Criar uma relação unificada de proteção de dados para o FlexGroup volumes

A partir do ONTAP 9.3, você pode criar e configurar relações de proteção de dados unificadas do SnapMirror para configurar a recuperação de desastres e o arquivamento no mesmo volume de destino.

O que você vai precisar

Você precisa estar ciente das considerações para criar relacionamentos de proteção de dados unificados para volumes do FlexGroup.

"Considerações para criar uma relação de backup do SnapVault e uma relação de proteção de dados unificada para volumes do FlexGroup"

Passos

1. Crie um volume FlexGroup de destino do tipo `DP` que tenha o mesmo número de constituintes do volume FlexGroup de origem:
   a. A partir do cluster de origem, determine o número de componentes no volume FlexGroup de origem: `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume         Aggregate    State      Type       Size
Available  Used%
--------- ------------   ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. A partir do cluster de destino, crie um volume do tipo FlexGroup de destino `DP` com o mesmo número de componentes que o do volume FlexGroup de origem.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. A partir do cluster de destino, verifique o número de componentes no volume FlexGroup de destino: `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     RW         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. Criar uma agenda de trabalhos: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para as `-month` opções , `-dayofweek`, e `-hour` , é possível especificar `all` para executar o trabalho todos os meses, todos os dias da semana e a cada hora, respetivamente.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. Crie uma política personalizada de tipo `mirror-vault` e defina uma regra para a política de espelhamento e cofre:

   a. Crie uma política de tipo personalizada `mirror-vault` para o relacionamento unificado de proteção de dados: `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`

   b. Defina uma regra para a política de espelhamento e cofre que determina quais cópias snapshot serão transferidas durante as operações de inicialização e atualização: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Se você não especificar uma política personalizada, a `MirrorAndVault` política será usada para relacionamentos de proteção de dados unificados.

4. Criar uma relação unificada de proteção de dados: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

   No ONTAP 9.4 e anteriores, se a política não for especificada com o `snapmirror create` comando, a `MirrorAllSnapshots` política será usada por padrão. No ONTAP 9.5, se a política não for especificada com o `snapmirror create` comando, a `MirrorAndVault` política será usada por padrão.

   ```
   cluster2::> snapmirror create -source-path vss:srcFG -destination-path
   vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
   ```

5. No cluster de destino, inicialize a relação unificada de proteção de dados executando uma transferência de linha de base: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror initialize -destination-path vsd:dstFG
   Operation is queued: snapmirror initialize of destination "vsd:dstFG".
   ```

Criar uma relação de recuperação de desastres do SVM para FlexGroup volumes

A partir do ONTAP 9.9,1, você pode criar relacionamentos de recuperação de desastres (SVM DR) usando o FlexGroup volumes. Uma relação SVM DR fornece redundância e a capacidade de recuperar FlexGroups em caso de desastre, sincronizando e replicando a configuração SVM e seus dados. É necessária uma licença SnapMirror para o SVM DR.

Antes de começar

Você *não pode* criar uma relação de DR do FlexGroup SVM com o seguinte se aplica.

- Existe uma configuração FlexClone FlexGroup
- O volume FlexGroup faz parte de uma relação em cascata
- O volume FlexGroup faz parte de uma relação de fanout, e seu cluster está executando uma versão do ONTAP anterior ao ONTAP 9.12,1. (Começando com ONTAP 9.13,1, relacionamentos de fanout são suportados.)

Sobre esta tarefa

- Todos os nós nos dois clusters precisam estar executando a mesma versão do ONTAP que o nó no qual foi adicionado suporte à SVM DR (ONTAP 9.9,1 ou posterior).
- A relação do SVM DR entre os locais primário e secundário deve estar saudável e ter espaço suficiente nas SVMs primárias e secundárias para dar suporte aos volumes FlexGroup.
- A partir do ONTAP 9.12,1, o FabricPool, o FlexGroup e o SVM DR podem funcionar em conjunto. Em versões anteriores ao ONTAP 9.12,1, quaisquer dois desses recursos funcionaram juntos, mas não todos os três em conjunto.
- Quando você cria uma relação de DR do FlexGroup SVM na qual o volume FlexGroup faz parte de uma relação de fanout, você deve estar ciente dos seguintes requisitos:

- O cluster de origem e destino deve estar executando o ONTAP 9.13,1 ou posterior.
- O SVM DR com FlexGroup volumes dá suporte a relacionamentos de fanout da SnapMirror em oito locais.

Para obter informações sobre como criar uma relação de SVM DR, "Gerenciar a replicação do SnapMirror SVM"consulte .

Passos

1. Crie uma relação SVM DR ou use uma relação existente.

   "Replique toda uma configuração da SVM"

2. Crie um volume FlexGroup no local principal com o número necessário de componentes.

   "Criando um volume FlexGroup".

   Aguarde até que o FlexGroup e todos os seus constituintes sejam criados antes de prosseguir.

3. Para replicar o volume FlexGroup, atualize o SVM no local secundário: `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

   Você também pode verificar se já existe uma atualização agendada do SnapMirror entrando `snapmirror show -fields schedule`

4. A partir do site secundário, verifique se a relação SnapMirror está saudável: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                 Idle           -         true    -
```

5. A partir do local secundário, verifique se o novo volume FlexGroup e seus constituintes existem: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                            Snapmirrored
                                Idle           -         true    -
6 entries were displayed.
```

Faça a transição de uma relação existente da FlexGroup SnapMirror para o SVM DR

Você pode criar uma relação de recuperação de desastres do SVM do FlexGroup fazendo a transição de uma relação existente do FlexGroup volume SnapMirror.

O que você vai precisar

- A relação FlexGroup volume SnapMirror está em um estado saudável.
- Os volumes FlexGroup de origem e destino têm o mesmo nome.

Passos

1. A partir do destino SnapMirror, ressincronize a relação FlexGroup Level SnapMirror: `snapmirror resync`

2. Criar a relação do FlexGroup SVM DR SnapMirror. Use a mesma política de SnapMirror configurada nas relações de SnapMirror de volume do FlexGroup: `snapmirror create -destination-path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`

   > Você deve usar a `-identity-preserve true` opção `snapmirror create` do comando ao criar sua relação de replicação.

3. Verifique se o relacionamento está quebrado: `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:


Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
fg_vs:        XDP  fg_vs1_renamed:     Broken-off
                                      Idle           -         true    -
```

4. Pare o SVM de destino: `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. Ressincronizar a relação SVM SnapMirror: `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. Verifique se a relação do SVM DR nível SnapMirror atinge um estado ocioso íntegro: `snapmirror show -expand`
7. Verifique se a relação FlexGroup SnapMirror está em um estado saudável: `snapmirror show`

Converter um FlexVol volume em um volume FlexGroup em uma relação SVM-DR

A partir do ONTAP 9.10,1, você pode converter um FlexVol volume em um volume FlexGroup em uma fonte SVM-DR.

O que você vai precisar

- O FlexVol volume que está sendo convertido deve estar on-line.
- As operações e configurações no FlexVol volume devem ser compatíveis com o processo de conversão.

  Uma mensagem de erro é gerada se o FlexVol volume tiver alguma incompatibilidade e a conversão de volume for cancelada. Você pode tomar ações corretivas e tentar novamente a conversão. Para obter mais detalhes, consulte "Considerações para converter volumes FlexVol para volumes FlexGroup"

Passos

1. Iniciar sessão utilizando o modo de privilégio avançado: `set -privilege advanced`
2. A partir do destino, atualize a relação SVM-DR:

   ```
   snapmirror update -destination-path <destination_svm_name>: -source-path
   <source_svm_name>:
   ```

   Você deve inserir dois pontos (:) após o nome SVM na `-destination-path` opção.

3. Certifique-se de que a relação SVM-DR esteja no estado com o SnapMirrored e não seja rompida:

   ```
   snapmirror show
   ```

4. No SVM de destino, verifique se o FlexVol volume está pronto para conversão:

   ```
   volume conversion start -vserver <svm_name> -volume <vol_name> -check
   -only true
   ```

   Se este comando gerar quaisquer erros que não "este é um volume SVMDR de destino", você pode tomar a ação corretiva apropriada, executar o comando novamente e continuar a conversão.

5. No destino, desative transferências na relação SVM-DR:

   ```
   snapmirror quiesce -destination-path <dest_svm>:
   ```

   Você deve inserir dois pontos (:) após o nome SVM na `-destination-path` opção.

6. No cluster de origem, inicie a conversão:

```
volume conversion start -vserver <svm_name> -volume <vol_name>
```

7. Verifique se a conversão foi bem-sucedida:

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state    volume-style-extended
-------  ---------  ------   ---------------------
vs0      my_volume  online   flexgroup
```

8. A partir do cluster de destino, retome as transferências para o relacionamento:

```
snapmirror resume -destination-path <dest_svm>:
```

> Você deve inserir dois pontos (:) após o nome SVM na `-destination-path` opção.

9. A partir do cluster de destino, execute uma atualização para propagar a conversão para o destino:

```
snapmirror update -destination-path <dest_svm>:
```

> Você deve inserir dois pontos (:) após o nome SVM na `-destination-path` opção.

10. Certifique-se de que a relação SVM-DR esteja no estado SnapMirrored e não seja interrompida:

```
snapmirror show
```

11. Certifique-se de que a conversão ocorreu no destino:

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state   volume-style-extended
-------  -------    ------  ---------------------
vs0_dst  my_volume  online  flexgroup
```

Considerações para criar relações de cascata e fanout do SnapMirror para FlexGroups

Existem considerações e limitações de suporte que você deve ter em mente ao criar relacionamentos em cascata e fanout do SnapMirror para volumes FlexGroup.

Considerações para criar relacionamentos em cascata

- Cada relacionamento pode ser um relacionamento inter cluster ou intra cluster.
- Todos os tipos de políticas assíncronas, incluindo async-mirror, mirror-Vault e Vault, são compatíveis com ambas as relações.
- Apenas as políticas "MirrorAllSnapshots" e não "MirrorLatest" async-mirror são suportadas.
- Atualizações simultâneas de relacionamentos XDP em cascata são suportadas.
- Suporta a remoção De A para B e B para C e ressincronizar A para C ou ressincronizar C para A.
- Os volumes a e B FlexGroup também suportam fanout quando todos os nós estão executando o ONTAP 9.9,1 ou posterior.
- As operações de restauração de volumes FlexGroup B ou C são compatíveis.
- Transferências em relacionamentos FlexGroup não são compatíveis enquanto o destino é a origem de um relacionamento de restauração.
- O destino de uma restauração do FlexGroup não pode ser o destino de qualquer outra relação do FlexGroup.
- As operações de restauração de arquivos do FlexGroup têm as mesmas restrições que as operações de restauração normais do FlexGroup.
- Todos os nós no cluster em que residem os volumes FlexGroup B e C devem estar executando o ONTAP 9.9,1 ou posterior.
- Todas as funcionalidades de expansão e expansão automática são suportadas.
- Em uma configuração em cascata, como A A B a C, se A a B e B a C tiverem números diferentes de relações SnapMirror constituintes, então uma operação de interrupção da fonte não é suportada para a relação B a C SnapMirror.
- O System Manager não oferece suporte a relacionamentos em cascata, independentemente da versão do ONTAP.
- Ao converter um conjunto de A para B para C de relação FlexVol para um relacionamento FlexGroup, você deve converter o B para C hop primeiro.
- Todas as configurações em cascata do FlexGroup para relacionamentos com tipos de política compatíveis com REST também são compatíveis com APIs REST em configurações de FlexGroup em cascata.
- Tal como acontece com as relações FlexVol, o FlexGroup em cascata não é suportado pelo `snapmirror protect` comando.

Considerações para criar relações de fanout

- Duas ou mais relações de fanout do FlexGroup são suportadas; por exemplo, A A B, A C, com um máximo de 8 pernas de fanout.
- Cada relacionamento pode ser entre clusters ou entre clusters.
- As atualizações simultâneas são suportadas para os dois relacionamentos.
- Todas as funcionalidades de expansão e expansão automática são suportadas.
- Se as pernas de fanout da relação têm números diferentes de relações SnapMirror constituintes, então

uma operação de abortar da fonte não é suportada para as relações A A B e A A C.

- Todos os nós do cluster onde residem os FlexGroups de origem e destino devem estar executando o ONTAP 9.9,1 ou posterior.
- Todos os tipos de políticas assíncronas atualmente suportados para FlexGroup SnapMirror são suportados em relacionamentos de fanout.
- Você pode executar operações de restauração de B para C FlexGroups.
- Todas as configurações de fanout com tipos de política suportados por REST também são suportadas para APIs REST em configurações de fanout do FlexGroup.

Considerações para criar uma relação de backup do SnapVault e uma relação de proteção de dados unificada para volumes do FlexGroup

Você precisa estar ciente das considerações para criar uma relação de backup da SnapVault e uma relação unificada de proteção de dados para volumes do FlexGroup.

- Você pode ressincronizar uma relação de backup do SnapVault e uma relação unificada de proteção de dados usando a `-preserve` opção que permite preservar cópias Snapshot no volume de destino mais recente que a cópia Snapshot comum mais recente.
- A retenção de longo prazo não é compatível com volumes FlexGroup.

  A retenção de longo prazo permite a criação de cópias Snapshot diretamente no volume de destino sem a necessidade de armazenar as cópias Snapshot no volume de origem.

- A `snapshot` opção de comando `expiry-time` não é suportada para volumes FlexGroup.
- A eficiência de storage não pode ser configurada no volume FlexGroup de destino de uma relação de backup da SnapVault e no relacionamento unificado de proteção de dados.
- Você não pode renomear cópias Snapshot de uma relação de backup do SnapVault e de proteção de dados unificada para volumes do FlexGroup.
- Um volume FlexGroup pode ser o volume de origem de apenas uma relação de backup ou restauração.

  Um volume FlexGroup não pode ser a origem de duas relações SnapVault, duas relações de restauração ou uma relação de backup SnapVault e uma relação de restauração.

- Se você excluir uma cópia Snapshot no volume FlexGroup de origem e recriar uma cópia Snapshot com o mesmo nome, a próxima transferência de atualização para o volume FlexGroup de destino falhará se o volume de destino tiver uma cópia Snapshot do mesmo nome.

  Isso ocorre porque as cópias Snapshot não podem ser renomeadas para volumes FlexGroup.

Monitore transferências de dados do SnapMirror para volumes do FlexGroup

Você deve monitorar periodicamente o status das relações do FlexGroup volume SnapMirror para verificar se o volume do FlexGroup de destino é atualizado periodicamente de acordo com a programação especificada.

Sobre esta tarefa

Tem de executar esta tarefa a partir do cluster de destino.

Passos

1. Exibir o status da relação SnapMirror de todas as relações de volume do FlexGroup: `snapmirror show -relationship-group-type flexgroup`

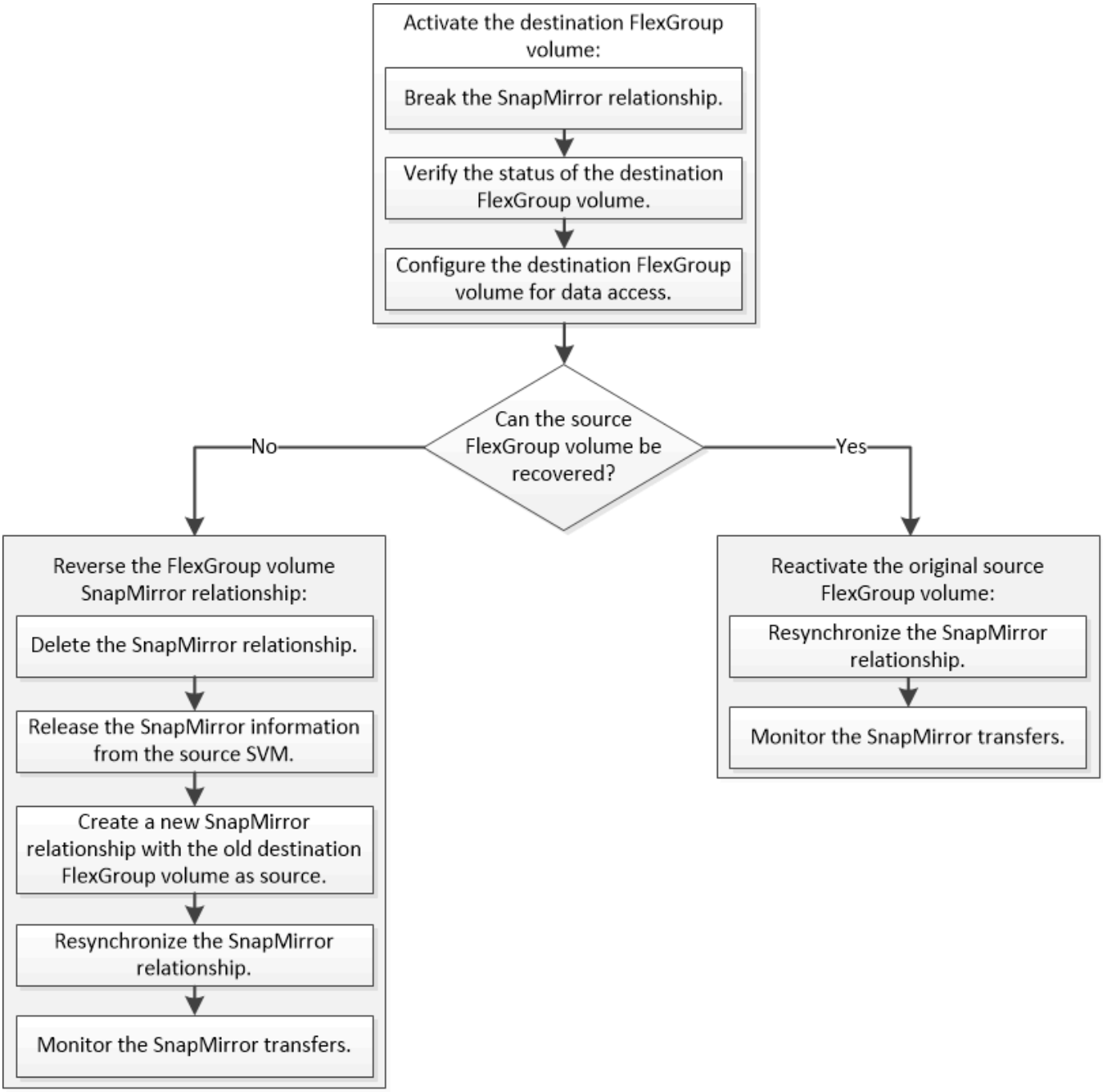
```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:d        Snapmirrored
                                    Idle           -         true    -
vss:s2      XDP  vsd:d2       Uninitialized
                                    Idle           -         true    -
2 entries were displayed.
```

Gerenciar operações de proteção de dados no FlexGroup volumes

Recuperação de desastres para FlexGroup volumes

Fluxo de trabalho de recuperação de desastres para FlexGroup volumes

Quando um desastre ocorre no volume FlexGroup de origem, você deve ativar o volume FlexGroup de destino e redirecionar o acesso do cliente. Dependendo se o volume FlexGroup de origem pode ser recuperado, você deve reativar o volume FlexGroup de origem ou reverter a relação SnapMirror.



Sobre esta tarefa

O acesso do cliente ao volume FlexGroup de destino é bloqueado por um breve período quando algumas operações do SnapMirror, como SnapMirror Break e ressincronização, estão em execução. Se a operação SnapMirror falhar, é possível que alguns dos constituintes permaneçam neste estado e o acesso ao volume FlexGroup seja negado. Nesses casos, você deve tentar novamente a operação SnapMirror.

Ative o volume FlexGroup de destino

Quando o volume FlexGroup de origem não conseguir fornecer dados devido a eventos como corrupção de dados, exclusão acidental ou estado offline, você deve ativar o volume FlexGroup de destino para fornecer acesso aos dados até que você recupere os dados no volume FlexGroup de origem. A ativação envolve parar futuras transferências de dados do SnapMirror e quebrar o relacionamento do SnapMirror.

Sobre esta tarefa

Tem de executar esta tarefa a partir do cluster de destino.

Passos

1. Desativar transferências futuras para a relação FlexGroup volume SnapMirror: `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. Quebre a relação SnapMirror do volume FlexGroup: `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. Veja o status da relação SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Broken-off
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Broken-off
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Broken-off
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Broken-off
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Broken-off
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Broken-off
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Broken-off
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Broken-off
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Broken-off
                                    Idle           -         true    -
...
```

O status da relação SnapMirror de cada componente é `Broken-off`.

4. Verifique se o volume FlexGroup de destino é leitura/gravação: `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     **RW**          2GB
1.54GB   22%
vsd       d2           -            online     DP           2GB
1.55GB   22%
vsd       root_vs0     aggr1        online     RW        100MB
94.02MB    5%
3 entries were displayed.
```

5. Redirecione os clientes para o volume FlexGroup de destino.

Reative o volume original do FlexGroup após o desastre

Quando o volume FlexGroup de origem ficar disponível, é possível ressincronizar os volumes FlexGroup de origem e destino originais. Todos os novos dados no volume FlexGroup de destino são perdidos.

Sobre esta tarefa

Todas as regras de quota ativas no volume de destino são desativadas e as regras de quota são eliminadas antes de ser efetuada a ressincronização.

Você pode usar os `volume quota policy rule create` comandos e `volume quota modify` para criar e reativar regras de cota após a conclusão da operação de ressincronização.

Passos

1. A partir do cluster de destino, ressincronize a relação SnapMirror volume FlexGroup: `snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. Veja o status da relação SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Snapmirrored
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Snapmirrored
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Snapmirrored
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Snapmirrored
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Snapmirrored
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Snapmirrored
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Snapmirrored
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Snapmirrored
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Snapmirrored
                                    Idle           -         true    -
...
```

O status da relação SnapMirror de cada componente é `Snapmirrored`.

Inverta uma relação do SnapMirror entre o FlexGroup volumes durante a recuperação de desastres

Quando um desastre desativa o volume FlexGroup de origem de uma relação SnapMirror, você pode usar o volume FlexGroup de destino para fornecer dados enquanto você reparar ou substituir o volume FlexGroup de origem. Depois que o volume FlexGroup de origem estiver on-line, você poderá fazer do volume FlexGroup de origem original um destino somente leitura e reverter a relação SnapMirror.

Sobre esta tarefa

Todas as regras de quota ativas no volume de destino são desativadas e as regras de quota são eliminadas antes de ser efetuada a ressincronização.

Você pode usar os `volume quota policy rule create` comandos e `volume quota modify` para criar e reativar regras de cota após a conclusão da operação de ressincronização.

Passos

1. No volume FlexGroup de destino original, remova a relação do espelho de proteção de dados entre o volume FlexGroup de origem e o volume FlexGroup de destino: `snapmirror delete -destination -path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. No volume FlexGroup de origem original, remova as informações de relacionamento do volume FlexGroup de origem: `snapmirror release -destination-path svm_name:volume_name -relationship-info-only`

   Depois de excluir um relacionamento SnapMirror, você deve remover as informações do relacionamento do volume FlexGroup de origem antes de tentar uma operação de ressincronização.

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship
-info-only true
```

3. No novo volume FlexGroup de destino, crie a relação de espelhamento: `snapmirror create -source -path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path
vss:src -type XDP -policy MirrorAllSnapshots
```

4. No novo volume FlexGroup de destino, ressincronize o FlexGroup de origem: `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. Monitorar as transferências do SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vsd:dst       XDP  vss:src        Snapmirrored
                                      Idle           -         true    -
vss:dst__0001 XDP  vss:src__0001  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0002 XDP  vss:src__0002  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0003 XDP  vss:src__0003  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0004 XDP  vss:src__0004  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0005 XDP  vss:src__0005  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0006 XDP  vss:src__0006  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0007 XDP  vss:src__0007  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0008 XDP  vss:src__0008  Snapmirrored
                                      Idle           -         true    -
...
```

O status da relação SnapMirror de cada constituinte mostra como `Snapmirrored` isso indica que a ressincronização foi bem-sucedida.

Expanda volumes do FlexGroup em uma relação do SnapMirror

Expanda volumes do FlexGroup em uma relação do SnapMirror

A partir do ONTAP 9.3, é possível expandir o volume FlexGroup de origem e o volume FlexGroup de destino que estão em uma relação do SnapMirror adicionando novos constituintes aos volumes. Pode expandir os volumes de destino manualmente ou automaticamente.

Sobre esta tarefa

- Após a expansão, o número de componentes no volume FlexGroup de origem e no volume FlexGroup de destino de uma relação SnapMirror deve corresponder.

  Se o número de componentes nos volumes não corresponder, as transferências SnapMirror falharão.

- Você não deve executar nenhuma operação SnapMirror quando o processo de expansão estiver em andamento.
- Se um desastre ocorrer antes que o processo de expansão seja concluído, você deve quebrar o relacionamento do SnapMirror e esperar até que a operação seja bem-sucedida.

> Você deve quebrar o relacionamento do SnapMirror quando o processo de expansão estiver em andamento apenas no caso de um desastre. No caso de um desastre, a operação de interrupção pode levar algum tempo para ser concluída. Você deve esperar que a operação de interrupção seja concluída com êxito antes de executar uma operação ressincronizada. Se a operação de interrupção falhar, você deve tentar novamente a operação de interrupção. Se a operação de quebra falhar, alguns dos novos constituintes poderão permanecer no volume FlexGroup de destino após a operação de quebra. É melhor excluir esses constituintes manualmente antes de prosseguir.

Expanda o volume FlexGroup de origem de uma relação SnapMirror

A partir do ONTAP 9.3, é possível expandir o volume FlexGroup de origem de uma relação do SnapMirror adicionando novos constituintes ao volume de origem. Você pode expandir o volume de origem da mesma forma que expande um volume FlexGroup normal (volume de leitura e gravação).

Passos

1. Expanda o volume FlexGroup de origem: `volume expand -vserver vserver_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src

Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
Partial Snapshot copies cannot be restored.
Do you want to continue? {y|n}: Y
[Job 146] Job succeeded: Successful
```

   O estado de todas as cópias Snapshot obtidas antes do volume é alterado para parcial.

Expanda o volume FlexGroup de destino de uma relação SnapMirror

Você pode expandir o volume FlexGroup de destino e restabelecer a relação SnapMirror automaticamente ou manualmente. Por padrão, a relação SnapMirror é definida para expansão automática e o volume FlexGroup de destino se expande automaticamente se o volume de origem for expandido.

O que você vai precisar

- O volume FlexGroup de origem deve ter sido expandido.
- A relação SnapMirror deve estar `SnapMirrored` no estado.

  A relação SnapMirror não deve ser quebrada ou excluída.

Sobre esta tarefa

- Quando o volume FlexGroup de destino é criado, o volume é configurado para expansão automática por padrão.

  Pode modificar o volume FlexGroup de destino para expansão manual, se necessário.

  A prática recomendada é expandir o volume FlexGroup de destino automaticamente.

- Todas as operações do SnapMirror falham até que o volume FlexGroup de origem e o volume FlexGroup de destino tenham expandido e tenham o mesmo número de componentes.
- Se você expandir o volume FlexGroup de destino depois que a relação SnapMirror for interrompida ou excluída, não será possível sincronizar novamente a relação original.

  Se pretender reutilizar o volume FlexGroup de destino, não deve expandir o volume depois de eliminar a relação SnapMirror.

Opções

- Execute uma transferência de atualização para expandir automaticamente o volume FlexGroup de destino:

  a. Execute uma transferência de atualização do SnapMirror: `snapmirror update -destination -path svm:vol_name`

  b. Verifique se o status da relação SnapMirror está no `SnapMirrored` estado: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

  Com base no tamanho e disponibilidade dos agregados, os agregados são selecionados automaticamente e novos constituintes que correspondem aos constituintes do volume FlexGroup de origem são adicionados ao volume FlexGroup de destino. Após a expansão, uma operação de ressincronização é

acionada automaticamente.

- Expanda o volume FlexGroup de destino manualmente:
  a. Se a relação SnapMirror estiver no modo de expansão automática, defina a relação SnapMirror para o modo de expansão manual: `snapmirror modify -destination-path svm:vol_name -is -auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

  b. Quiesce a relação de SnapMirror: `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

  c. Expanda o volume FlexGroup de destino: `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2  -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

  d. Ressincronizar a relação SnapMirror: `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

  e. Verifique se o status da relação SnapMirror é `SnapMirrored`: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

Execute uma restauração de arquivo único do SnapMirror a partir de um volume do FlexGroup

A partir do ONTAP 9.8, você pode restaurar um único arquivo a partir de um cofre FlexGroup SnapMirror ou de um destino UDP.

Sobre esta tarefa

- Você pode restaurar de um volume FlexGroup de qualquer geometria para o volume FlexGroup de qualquer geometria
- Apenas um arquivo por operação de restauração é suportado
- Você pode restaurar o volume FlexGroup de origem original ou um novo volume FlexGroup
- A pesquisa remota de ficheiros vedada não é suportada.

  A restauração de um único arquivo falha se o arquivo de origem estiver cercado.

- Você pode reiniciar ou limpar uma restauração de arquivo único abortada
- Você deve limpar uma transferência de restauração de arquivo único com falha usando a `clean-up-failure` opção `snapmirror restore` do comando
- A expansão de volumes FlexGroup é suportada quando uma restauração de arquivo único FlexGroup está em andamento ou em um estado abortado

Passos

1. Restaurar um arquivo a partir de um volume FlexGroup:`snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

   A seguir está um exemplo de uma operação de restauração de arquivo único de volume FlexGroup.

   ```
   vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path
   vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-
   d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
   ```

```
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631.
vserverA::> snapmirror show

Source              Destination Mirror   Relationship
Total Last
Path       Type   Path            State    Status           Progress
Healthy Updated
---------- ----      ------------     -------    ---------
----- --------- ------- --------
vs0:v1d RST    vs0:v2          -           Transferring Idle 83.12KB
true 09/19 11:38:42

vserverA::*> snapmirror show vs0:fg2

Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
```

```
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

Restaurar um volume FlexGroup a partir de um backup do SnapVault

Você pode executar uma operação de restauração de volume total dos volumes do FlexGroup a partir de uma cópia Snapshot no volume secundário do SnapVault. Você

pode restaurar o volume FlexGroup para o volume de origem original ou para um novo volume FlexGroup.

Antes de começar

Você precisa estar ciente de alguns considerações ao restaurar os backups do SnapVault para volumes FlexGroup.

- Somente a restauração de linha de base é compatível com cópias Snapshot parciais de um backup do SnapVault. O número de constituintes no volume de destino deve corresponder ao número de constituintes no volume de origem quando a cópia Snapshot foi obtida.
- Se uma operação de restauração falhar, nenhuma outra operação será permitida até que a operação de restauração esteja concluída. Você pode tentar novamente a operação de restauração ou executar a operação de restauração com o `cleanup` parâmetro.
- Um volume FlexGroup pode ser o volume de origem de apenas uma relação de backup ou restauração. Um volume FlexGroup não pode ser a origem de duas relações SnapVault, duas relações de restauração ou uma relação SnapVault e uma relação de restauração.
- As operações de backup e restauração do SnapVault não podem ser executadas em paralelo. Quando uma operação de restauração de linha de base ou uma operação de restauração incremental estiverem em andamento, você deverá desativar as operações de backup.
- É necessário cancelar uma operação de restauração de uma cópia Snapshot parcial do volume FlexGroup de destino. Não é possível cancelar a operação de restauração de uma cópia Snapshot parcial do volume de origem.
- Se você cancelar uma operação de restauração, será necessário reiniciar a operação de restauração com a mesma cópia Snapshot usada para a operação de restauração anterior.

Sobre esta tarefa

Todas as regras de cota ativa no volume FlexGroup de destino são desativadas antes da restauração ser executada.

Você pode usar o `volume quota modify` comando para reativar regras de cota após a conclusão da operação de restauração.

Passos

1. Restaurar o volume FlexGroup: `snapmirror restore -source-path` *`src_svm:src_flexgroup`* `-destination-path` *`dest_svm:dest_flexgroup`* `-snapshot` *`snapshot_name`* `snapshot_name` É a cópia Snapshot que deve ser restaurada do volume de origem para o volume de destino. Se a cópia Snapshot não for especificada, o volume de destino será restaurado a partir da cópia Snapshot mais recente.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

Desativar a proteção contra SVM em um volume FlexGroup

Quando o sinalizador SVM DR está definido como `protected` em um volume

FlexGroup, você pode definir o sinalizador como desprotegido para desativar o SVM DR `protection` em um volume FlexGroup.

O que você vai precisar

- A relação do SVM DR entre o primário e o secundário está saudável.
- O parâmetro de proteção do SVM DR é definido como `protected`.

Passos

1. Desative a proteção usando o `volume modify` comando para alterar o `vserver-dr-protection` parâmetro do volume FlexGroup para `unprotected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Atualize o SVM no local secundário: `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. Verifique se a relação SnapMirror está saudável: `snapmirror show`
4. Verifique se a relação FlexGroup SnapMirror foi removida: `snapmirror show -expand`

Ativar a proteção contra SVM em um volume FlexGroup

Quando o sinalizador de proteção do SVM DR está definido como `unprotected` em um volume FlexGroup, você pode definir o sinalizador para `protected` habilitar a proteção contra SVM DR.

O que você vai precisar

- A relação do SVM DR entre o primário e o secundário está saudável.
- O parâmetro de proteção do SVM DR é definido como `unprotected`.

Passos

1. Ative a proteção utilizando o `volume modify` para alterar o `vserver-dr-protection` parâmetro do volume FlexGroup para `protected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Atualize o SVM no local secundário: `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. Verifique se a relação SnapMirror está saudável: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                   Idle           -         true    -
```

4. Verifique se a relação FlexGroup SnapMirror está saudável: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                            Snapmirrored
                                Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                            Snapmirrored
                                Idle           -         true    -
6 entries were displayed.
```

Converter volumes FlexVol em volumes FlexGroup

Visão geral da conversão de volumes FlexVol para volumes FlexGroup

Se você quiser expandir um FlexVol volume além do limite de espaço, você pode converter o FlexVol volume em um volume FlexGroup. A partir do ONTAP 9.7, você pode converter volumes FlexVol autônomos ou volumes FlexVol que estão em uma relação do SnapMirror para volumes do FlexGroup.

Considerações para converter volumes FlexVol para volumes FlexGroup

Você deve estar ciente dos recursos e operações com suporte antes de decidir converter volumes do FlexVol para volumes do FlexGroup.

A partir do ONTAP 9.13,1, a proteção autônoma contra ransomware pode permanecer habilitada durante as conversões. Se a proteção estiver ativa, o FlexVol original se tornará o componente raiz FlexGroup após a conversão. Se a proteção estiver inativa, um novo FlexGroup será criado durante a conversão e o FlexVol original assumirá o papel de componente raiz.

Operações não suportadas durante a conversão

As seguintes operações não são permitidas quando a conversão de volume está em andamento:

- Movimentação de volume
- Agregar o equilíbrio automático
- Realocação de agregados
- Takeover planejado e giveback em uma configuração de alta disponibilidade
- Giveback manual e automático em uma configuração de alta disponibilidade
- Atualização e reversão do cluster
- Divisão de volume FlexClone
- Rehost de volume
- Modificação de volume e dimensionamento automático
- Mudar o nome do volume
- Anexando um armazenamento de objetos a um agregado
- Switchover negociado na configuração do MetroCluster
- Operações da SnapMirror
- Restaurar a partir de uma cópia Snapshot
- Operações de cota
- Operações de eficiência de storage

Você pode executar essas operações no volume FlexGroup após a conversão bem-sucedida.

Configurações que não são compatíveis com o FlexGroup volumes

- Volume off-line ou restrito
- Volume raiz do SVM
- SAN
- SMB 1,0
- Namespaces NVMe
- Serviço de cópia de sombra de volume remoto (VSS)

Converter um FlexVol volume em um volume FlexGroup

A partir do ONTAP 9.7, você pode executar uma conversão no local de um FlexVol volume para um volume FlexGroup sem exigir uma cópia de dados ou espaço em disco adicional.

Antes de começar

- Os volumes transferidos podem ser convertidos para volumes FlexGroup a partir do ONTAP 9.8.
- O FlexVol volume que está sendo convertido deve estar on-line.
- As operações e configurações no FlexVol volume devem ser compatíveis com o processo de conversão.

  Verifique se existem as seguintes condições que podem impedir que a conversão seja bem-sucedida:

  - Um FlexVol volume foi transferido do modo 7 usando 7MTT (ONTAP 9.7).

    Os volumes transicionados podem ser convertidos a partir de ONTAP 9.8.

  - Algo está ativado no volume que ainda não é compatível com o volume FlexGroup; por exemplo, LUNs SAN, Windows NFS, SMB1, Snapshot naming/slip, vmalign Set, SnapLock, SLO de espaço ou imposição/geração de relatórios de espaço lógico. Para obter mais informações, "Configurações com suporte e sem suporte para volumes FlexGroup"consulte .
  - O SVM DR no momento, o FlexVol volume a ser convertido está usando o SVM DR.
  - Os volumes NetApp FlexClone estão presentes e o FlexVol volume é o volume pai. O volume que está sendo convertido não pode ser um pai ou um clone.
  - O volume é um volume de origem NetApp FlexCache.
  - Para o ONTAP 9.7 e versões anteriores, as cópias Snapshot do NetApp não devem ser superiores a 255. Para o ONTAP 9.8 e posterior, há suporte para cópias Snapshot de 1023.
  - As eficiências de storage são habilitadas. Estes devem ser desativados e podem ser reativados após a conversão.
  - O volume é uma fonte de um relacionamento SnapMirror e o destino ainda não foi convertido.
  - O volume faz parte de uma relação SnapMirror ativa (não quiesced).
  - As quotas estão ativadas. Estes devem ser desativados e podem ser reativados após a conversão.
  - Os nomes dos volumes têm mais de 197 carateres.
  - O volume está associado a uma aplicação.

    Isto é aplicável apenas ao ONTAP 9.7. A limitação é removida no ONTAP 9.8.

  - Os processos do ONTAP estão em execução, como espelhamento, tarefas, wafliron, backup NDMP e conversão de inode em processo.
  - O volume é um volume raiz da SVM.
  - O volume está demasiado cheio.

    Se alguma dessas incompatibilidades existir, uma mensagem de erro será gerada se o FlexVol volume e a conversão de volume for abortada. Você pode tomar ações corretivas e tentar novamente a conversão.

- Se um FlexVol volume estiver atualmente com 80% ou mais de capacidade máxima, considere copiar os dados para um volume FlexGroup recém-criado em vez de executar uma conversão no local. Embora os volumes membros do FlexGroup reequilibrem naturalmente com o tempo, ao converter um FlexVol volume de alta capacidade em um volume de FlexGroup pode criar problemas de performance ou equilíbrio que não serão rebalanceados rapidamente nos volumes dos membros.

Converter um volume FlexGroup muito grande resulta em um componente membro do volume FlexGroup muito completo, o que pode criar problemas de desempenho. Para obter mais informações, consulte a seção chamada "quando não criar um volume FlexGroup" no "FlexGroup volumes - Guia de práticas recomendadas e implementação"TR .

Passos

1. Verifique se o FlexVol volume está online: `volume show vol_name volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexvol
```

2. Verifique se o FlexVol volume pode ser convertido sem problemas:

   a. Inicie sessão no modo de privilégio avançado: `set -privilege advanced`

   b. Verifique o processo de conversão: `volume conversion start -vserver vs1 -volume flexvol -check-only true`

   Você deve corrigir todos os erros antes de converter o volume.

   Não é possível converter um volume FlexGroup de volta para um FlexVol volume.

3. Inicie a conversão: `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion Snapshot copies cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. Verifique se a conversão foi bem-sucedida: `volume show vol_name -fields volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexgroup
```

Resultados

O FlexVol volume é convertido em um volume FlexGroup de membro único.

Depois de terminar

Você pode expandir o volume FlexGroup, conforme necessário.

Converta uma relação FlexVol volume SnapMirror para uma relação FlexGroup volume SnapMirror

Para converter uma relação FlexVol volume SnapMirror para uma relação FlexGroup volume SnapMirror no ONTAP, primeiro você deve converter o FlexVol volume de destino seguido do FlexVol volume de origem.

Sobre esta tarefa

- A conversão FlexGroup é suportada apenas para relacionamentos assíncronos do SnapMirror.
- O tempo de conversão depende de várias variáveis. Algumas das variáveis incluem:
  - CPU do controlador
  - Utilização da CPU por outras aplicações
  - Quantidade de dados na cópia Snapshot inicial
  - Largura de banda da rede
  - Largura de banda utilizada por outras aplicações

Antes de começar

- O FlexVol volume que está sendo convertido deve estar on-line.
- O FlexVol volume de origem no relacionamento SnapMirror não deve ser o volume de origem para vários relacionamentos SnapMirror.

  A partir do ONTAP 9.9,1, as relações de fanout SnapMirror são suportadas para volumes FlexGroup. Para obter mais informações, "Considerações para criar relações de cascata e fanout do SnapMirror para FlexGroups"consulte .

- As operações e configurações no FlexVol volume devem ser compatíveis com o processo de conversão.

  Uma mensagem de erro é gerada se o FlexVol volume tiver alguma incompatibilidade e a conversão de volume for abortada. Você pode tomar ações corretivas e tentar novamente a conversão.

Passos

1. Verifique se a relação SnapMirror está saudável:

```
snapmirror show
```

Apenas as relações de espelho do tipo XDP podem ser convertidas.

Exemplo:

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:src_dpv DP   vs2:dst_dpv  Snapmirrored
                                     Idle           -         true    -
vs0:src_xdp XDP  vs2:dst_xdp  Snapmirrored
                                     Idle           -         true    -
```

2. Verifique se o volume de origem é compatível para conversão:

   a. Inicie sessão no modo de privilégio avançado:

      ```
      set -privilege advanced
      ```

   b. Verifique o processo de conversão:

      ```
      volume conversion start -vserver <src_svm_name> -volume <src_vol>
      -check-only true
      ```

      Exemplo:

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+
Você deve corrigir todos os erros antes de converter o volume.

3. Converta o FlexVol volume de destino para o volume FlexGroup.

   a. Quiesce a relação de FlexVol SnapMirror:

      ```
      snapmirror quiesce -destination-path <dest_svm:dest_volume>
      ```

      Exemplo:

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

b. Inicie a conversão:

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

Exemplo:

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp

Warning: After the volume is converted to a FlexGroup, it will not be
possible
to change it back to a flexible volume.
Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has
been successfully converted to a FlexGroup volume.
You must now convert the relationship's source volume, "vs0:src_xdp", to
a FlexGroup.
Then, re-establish the SnapMirror relationship using the "snapmirror
resync" command.
```

4. Converter o FlexVol volume de origem para FlexGroup volume: "

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

Exemplo:

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion Snapshot copies cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. Ressincronizar a relação:

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

Exemplo:

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

Depois de terminar

Certifique-se de que, quando o volume FlexGroup de origem for expandido para incluir mais constituintes, o volume de destino também será expandido.

Gerenciamento de volumes do FlexCache

Visão geral do FlexCache

A tecnologia NetApp FlexCache acelera o acesso aos dados, reduz a latência da WAN e reduz os custos de largura de banda da WAN para workloads com uso intenso de leitura, especialmente quando os clientes precisam acessar os mesmos dados repetidamente. Ao criar um volume FlexCache, você cria um cache remoto de um volume (origem) já existente que contém apenas os dados acessados ativamente (dados ativos) do volume de origem.

Quando um volume FlexCache recebe uma solicitação de leitura dos dados ativos que ele contém, ele pode responder mais rápido do que o volume de origem porque os dados não precisam viajar até o cliente. Se um volume FlexCache receber uma solicitação de leitura para dados de leitura com pouca frequência (dados inativos), ele recupera os dados necessários do volume de origem e armazena os dados antes de servir a solicitação do cliente. As solicitações de leitura subsequentes para esses dados são então fornecidas diretamente do volume FlexCache. Após a primeira solicitação, os dados não precisam mais viajar pela rede ou ser atendidos de um sistema carregado. Por exemplo, suponha que você esteja enfrentando gargalos no cluster em um ponto de acesso singular para dados solicitados com frequência. Você pode usar o FlexCache volumes no cluster para fornecer vários pontos de montagem nos dados ativos, reduzindo os gargalos e aumentando a performance. Como outro exemplo, suponha que você precise diminuir o tráfego de rede para um volume que é acessado de vários clusters. Você pode usar o FlexCache volumes para distribuir dados ativos do volume de origem entre os clusters da rede. Isso reduz o tráfego de WAN, dando aos usuários pontos de acesso mais próximos.

Você também pode usar a tecnologia FlexCache para melhorar a performance em ambientes de nuvem ou nuvem híbrida. Um volume FlexCache pode ajudar você a migrar workloads para a nuvem híbrida armazenando dados em cache de um data center local para a nuvem. Também é possível usar o FlexCache volumes para remover silos de nuvem, armazenando dados em cache de um fornecedor de nuvem para outro ou entre duas regiões do mesmo fornecedor de nuvem.

A partir do ONTAP 9.10,1, você pode "ative o bloqueio global de ficheiros" em todos os volumes do FlexCache. O bloqueio global de arquivos impede que um usuário acesse um arquivo que já esteja aberto por outro usuário. As atualizações do volume de origem são então distribuídas para todos os volumes FlexCache simultaneamente.

A partir do ONTAP 9.9,1, o FlexCache volumes mantém uma lista de arquivos não encontrados. Isso ajuda a reduzir o tráfego de rede removendo a necessidade de enviar várias chamadas para a origem quando os

clientes pesquisam arquivos inexistentes.

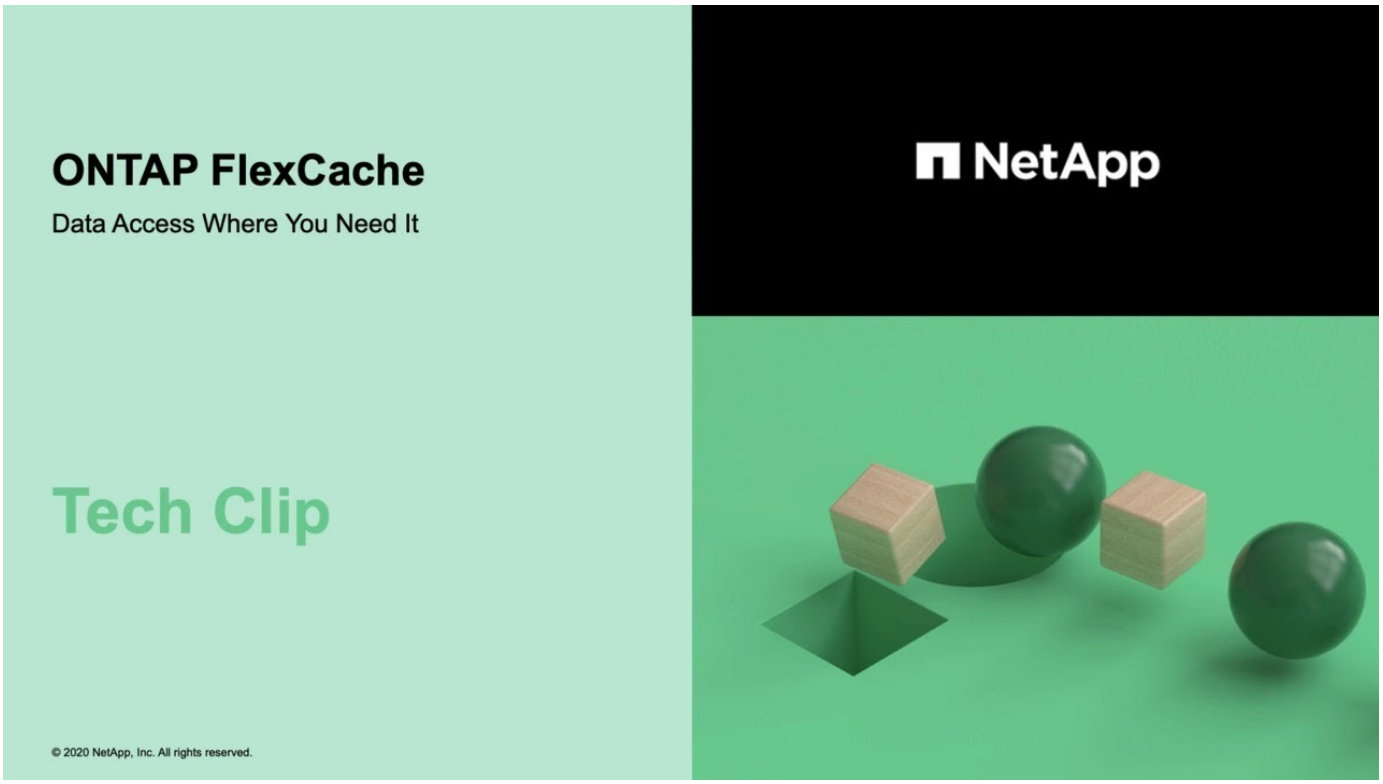
"Recursos compatíveis com volumes FlexCache e seus volumes de origem"Também está disponível uma lista de protocolos adicionais, incluindo uma lista de protocolos suportados pela versão ONTAP.

Você pode aprender mais sobre a arquitetura da tecnologia ONTAP FlexCache no "TR-4743: FlexCache em ONTAP".

Vídeos

Como o FlexCache pode reduzir a latência da WAN e os tempos de leitura para dados globais

Saiba mais sobre os benefícios de desempenho do ONTAP FlexCache!



Recursos suportados e não suportados para volumes FlexCache

A partir do ONTAP 9.5, você pode configurar volumes FlexCache. Os volumes FlexVol são compatíveis como volumes de origem, e os volumes FlexGroup são compatíveis com volumes FlexCache. A partir do ONTAP 9.7, tanto os volumes FlexVol quanto os volumes FlexGroup são suportados como volumes de origem. Os recursos e protocolos suportados para o volume de origem e o volume FlexCache variam.

Os volumes de cache e os volumes de origem podem interoperar desde que ambos estejam sendo executados em uma versão compatível do ONTAP. Tenha em mente que os recursos são suportados somente quando o cache e a origem estão executando pelo menos a versão ONTAP onde o suporte foi introduzido ou uma versão posterior do ONTAP.

Protocolos compatíveis

Protocolo	Suportado no volume Origin?	Compatível com o volume FlexCache?
NFSv3	Sim	Sim

NFSv4	Sim Para acessar volumes de cache usando o protocolo NFSv4.x, os clusters de origem e cache devem estar usando o ONTAP 9.10,1 ou posterior. O cluster de origem e o cluster FlexCache podem ter versões diferentes do ONTAP, mas ambos devem ser ONTAP 9.10,1 e versões posteriores, por exemplo, a origem pode ter ONTAP 9.10,1, e o cache pode ter ONTAP 9.11,1.	Sim Suportado a partir de ONTAP 9.10,1. Para acessar volumes de cache usando o protocolo NFSv4.x, os clusters de origem e cache devem estar usando o ONTAP 9.10,1 ou posterior. O cluster de origem e o cluster FlexCache podem ter versões diferentes do ONTAP, mas ambos devem ser ONTAP 9.10,1 e versões posteriores, por exemplo, a origem pode ter ONTAP 9.10,1, e o cache pode ter ONTAP 9.11,1.
NFSv4.2	Sim	Não
SMB	Sim	Sim Suportado a partir de ONTAP 9.8.

Recursos suportados

Recurso	Suportado no volume Origin?	Compatível com o volume FlexCache?
Proteção autônoma contra ransomware	Sim Compatível com volumes de origem FlexVol a partir de ONTAP 9.10,1 e compatível com volumes de origem FlexGroup a partir de ONTAP 9.13,1. "Casos de uso e considerações da proteção autônoma contra ransomware"Consulte .	Não

Antivírus	Sim Suportado a partir de ONTAP 9.7.	Não aplicável Se você configurar a verificação antivírus na origem, ela não será necessária no cache. A verificação do antivírus Origin deteta arquivos infetados com vírus antes que as gravações sejam confirmadas, independentemente da fonte de gravação. Para obter mais informações sobre como usar a verificação antivírus com o FlexCache, consulte "FlexCache com relatório técnico da ONTAP".
Auditoria	Sim Suportado a partir de ONTAP 9.7. É possível auditar eventos de acesso a arquivos NFS em relacionamentos do FlexCache com a auditoria nativa do ONTAP. Para obter mais informações, consulte Considerações para auditoria de volumes do FlexCache	Sim Suportado a partir de ONTAP 9.7. É possível auditar eventos de acesso a arquivos NFS em relacionamentos do FlexCache com a auditoria nativa do ONTAP. Para obter mais informações, consulte Considerações para auditoria de volumes do FlexCache
Cloud Volumes ONTAP	Sim Suportado a partir do ONTAP 9.6	Sim Suportado a partir do ONTAP 9.6
Compactação	Sim Suportado a partir do ONTAP 9.6	Sim Suportado a partir do ONTAP 9.7
Compactação	Sim Suportado a partir do ONTAP 9.6	Sim Suportado a partir do ONTAP 9.6
Deduplicação	Sim	Sim A deduplicação in-line é compatível com volumes FlexCache a partir de ONTAP 9.6. A deduplicação entre volumes é compatível com volumes do FlexCache a partir do ONTAP 9.7.
FabricPool	Sim	Sim Suportado a partir do ONTAP 9.7

FlexCache DR	Sim	Sim Suportado apenas a partir do ONTAP 9.9,1, com protocolo NFSv3. Os volumes do FlexCache devem estar em SVMs separadas ou em clusters separados.
Volume FlexGroup	Sim Suportado a partir do ONTAP 9.7	Sim
FlexVol volume	Sim	Não
FPolicy	Sim Suportado a partir do ONTAP 9.7	Sim Compatível com NFS a partir do ONTAP 9.7. Compatível com SMB a partir do ONTAP 9.14,1.
Configuração do MetroCluster	Sim Suportado a partir do ONTAP 9.7	Sim Suportado a partir do ONTAP 9.7
Microsoft offloaded Data Transfer (ODX)	Sim	Não
Criptografia de agregados NetApp (NAE)	Sim Suportado a partir do ONTAP 9.6	Sim Suportado a partir do ONTAP 9.6
Criptografia de volume NetApp (NVE)	Sim Suportado a partir do ONTAP 9.6	Sim Suportado a partir do ONTAP 9.6
Balde nas ONTAP S3	Sim Suportado a partir de ONTAP 9.12,1	Não
QoS	Sim	Sim A QoS em nível de arquivo não é suportada para volumes FlexCache.

Qtrees	Sim Começando com ONTAP 9.6, você pode criar e modificar qtrees. Qtrees criados na fonte podem ser acessados no cache.	Não
Quotas	Sim A partir do ONTAP 9.6, a aplicação de cotas nos volumes de origem do FlexCache é suportada para usuários, grupos e qtrees.	Não Com o modo FlexCache writearound (o modo padrão), as gravações no cache são encaminhadas para o volume de origem. As quotas são aplicadas na origem. A partir do ONTAP 9.6, a cota remota (rquota) é suportada em volumes FlexCache.
Change Notify SMB	Sim	Sim A partir do ONTAP 9.14,1, o SMB Change Notify é suportado no cache.
Volumes SnapLock	Não	Não
Relações assíncronas do SnapMirror*	Sim	Não

	• Origens do FlexCache: • Você pode ter um volume FlexCache de um Origin FlexVol • Você pode ter um volume FlexCache de um Origin FlexGroup • Você pode ter um volume FlexCache de um volume primário de origem no relacionamento SnapMirror. • Começando com ONTAP 9.8, um volume secundário SnapMirror pode ser um volume de origem FlexCache. O volume secundário do SnapMirror deve estar inativo sem atualizações ativas do SnapMirror; caso contrário, a criação do FlexCache falha.	Relações síncronas da SnapMirror
Não	Não	SnapRestore
Sim	Não	Cópias Snapshot
Sim	Não	Configuração de SVM DR
Sim Compatível a partir do ONTAP 9,5. O SVM principal de uma relação SVM DR pode ter o volume de origem. No entanto, se a relação SVM DR for interrompida, a relação FlexCache precisa ser recriada com um novo volume de origem.	Não Você pode ter volumes FlexCache em SVMs primárias, mas não em SVMs secundárias. Qualquer volume de FlexCache na SVM principal não é replicado como parte da relação SVM DR.	Proteção de acesso no nível de armazenamento (ESCÓRIA)
Não	Não	Thin Provisioning
Sim	Sim Suportado a partir do ONTAP 9.7	Clonagem de volume

Sim A clonagem de um volume de origem e dos arquivos no volume de origem é suportada a partir do ONTAP 9.6.	Não	Movimentação de volume
Sim	Sim (apenas para componentes de volume) A movimentação de componentes de volume de um volume FlexCache é suportada com o ONTAP 9.6 e posterior.	Rehost de volume
Não	Não	API vStorage para integração de array (VAAI)

Nas versões do ONTAP 9 anteriores a 9,5, os volumes do Origin FlexVol só podem servir dados para volumes do FlexCache criados em sistemas que executam o Data ONTAP 8.2.x operando no modo 7. A partir do ONTAP 9.5, o Origin FlexVol volumes também pode fornecer dados para o FlexCache volumes em sistemas ONTAP 9. Para obter informações sobre a migração do FlexCache de 7 modos para o ONTAP 9 FlexCache, "Relatório Técnico da NetApp 4743: FlexCache em ONTAP"consulte .

Diretrizes para dimensionamento de um volume FlexCache

Antes de começar a provisionar os volumes, você precisa estar ciente dos limites do FlexCache volumes.

O limite de tamanho de um FlexVol volume é aplicável a um volume de origem. O tamanho de um volume FlexCache pode ser menor ou igual ao volume de origem. A melhor prática para o tamanho de um volume de FlexCache é ser pelo menos 10% do tamanho do volume de origem.

Você também precisa estar ciente dos seguintes limites adicionais para o FlexCache volumes:

Limite	ONTAP 9,5-9,6	ONTAP 9,7	ONTAP 9 F.8 e mais tarde
Número máximo de volumes FlexCache que você pode criar a partir de um volume de origem	10	10	100
Número máximo recomendado de volumes de origem por nó	10	100	100
Número máximo recomendado de volumes FlexCache por nó	10	100	100
Número máximo recomendado de componentes FlexGroup em um volume FlexCache por nó	40	800	800
Número máximo de constituintes por volume FlexCache por nó	32	32	32

Informações relacionadas

"Interoperabilidade do NetApp"

Crie um volume FlexCache

Você pode criar um volume FlexCache no mesmo cluster para melhorar a performance ao acessar um objeto ativo. Se você tiver data centers em diferentes locais, poderá criar FlexCache volumes em clusters remotos para acelerar o acesso aos dados.

Sobre esta tarefa

- A partir do ONTAP 9.5, o FlexCache oferece suporte a volumes FlexVol como volumes de origem e volumes FlexGroup como volumes FlexCache.
- A partir do ONTAP 9.7, os volumes FlexVol volume e FlexGroup são compatíveis como volumes de origem.
- A partir do ONTAP 9.14,0, você pode criar um volume FlexCache não criptografado a partir de uma fonte criptografada.

Antes de começar

- Você deve estar executando o ONTAP 9.5 ou posterior.
- Se você estiver executando o ONTAP 9.6 ou anterior, você deve "Adicione uma licença FlexCache".

  Não é necessária uma licença FlexCache para o ONTAP 9.7 ou posterior. A partir do ONTAP 9.7, a funcionalidade FlexCache está incluída no ONTAP e não requer mais licença ou ativação.

> Se um par de HA estiver usando "Criptografia de unidades SAS ou NVMe (SED, NSE, FIPS)", siga as instruções no "Retornar uma unidade FIPS ou SED para o modo desprotegido"tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Exemplo 9. Passos

System Manager

1. Se o volume FlexCache estiver em um cluster diferente do volume de origem, crie uma relação de par de cluster:
   a. No cluster local, clique em **proteção > Visão geral**.
   b. Expanda **Intercluster Settings**, clique em **Add Network interfaces** e adicione interfaces de rede entre clusters para o cluster.

      Repita este passo no painel remoto.

   c. No cluster remoto, clique em **proteção > Visão geral**. Clique ⋮ na seção Cluster Peers e clique em **Generate Passphrase**.
   d. Copie a frase-passe gerada e cole-a no cluster local.
   e. No cluster local, em Cluster Peers, clique em **Peer clusters** e emparelhe os clusters locais e remotos.
2. Criar um relacionamento com colegas SVM:

   Em Storage VM Peers, clique ⋮ em e em **Peer Storage VMs** para fazer peer nas VMs de armazenamento.
3. Selecione **armazenamento > volumes**.
4. Selecione **Adicionar**.
5. Selecione **mais Opções** e, em seguida, selecione **Adicionar como cache para um volume remoto**.

   ⓘ Se você estiver executando o ONTAP 9.8 ou posterior e quiser desativar o QoS ou escolher uma política de QoS personalizada, clique em **mais opções** e, em **armazenamento e otimização**, selecione **nível de serviço de desempenho**.

CLI

1. Se o volume FlexCache a ser criado estiver em um cluster diferente, crie uma relação de par de cluster:
   a. No cluster de destino, crie uma relação de mesmo nível com o cluster de origem de proteção de dados:

      ```
      cluster peer create -generate-passphrase -offer-expiration
      MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
      <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
      -ipspace <ipspace_name>
      ```

      A partir do ONTAP 9.6, a criptografia TLS é ativada por padrão ao criar uma relação de par de cluster. A criptografia TLS é suportada para a comunicação entre clusters entre os volumes de origem e FlexCache. Você também pode desativar a criptografia TLS para o relacionamento de pares de cluster, se necessário.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

a. No cluster de origem, autentique o cluster de origem no cluster de destino:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. Se o volume FlexCache estiver em um SVM diferente daquele do volume de origem, crie um relacionamento de mesmo nível com `flexcache` o como aplicação:

a. Se o SVM estiver em um cluster diferente, crie uma permissão SVM para os SVMs de peering:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

O exemplo a seguir ilustra como criar uma permissão SVM peer que se aplica a todos os SVMs locais:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. Crie o relacionamento entre pares SVM:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Criar um volume FlexCache:

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

O exemplo a seguir cria um volume FlexCache e seleciona automaticamente agregados existentes para provisionamento:

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

O exemplo a seguir cria um volume FlexCache e define o caminho de junção:

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. Verifique a relação FlexCache a partir do volume FlexCache e do volume de origem.

a. Veja a relação do FlexCache no cluster:

```
volume flexcache show
```

```
cluster1::> volume flexcache show
Vserver Volume      Size       Origin-Vserver Origin-Volume
Origin-Cluster
------- ----------- ---------- -------------- -------------
--------------
vs_1    fc1         160MB      vs_1           vol_1
cluster1
```

b. Veja todas as relações FlexCache no cluster de origem
`volume flexcache origin show-caches`

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume   Cache-Vserver    Cache-Volume
Cache-Cluster
-------------- --------------- ---------------  --------------
---------------
vs0            ovol1           vs1              cfg1
clusA
vs0            ovol1           vs2              cfg2
clusB
vs_1           vol_1           vs_1             fc1
cluster1
```

Resultado

O volume FlexCache foi criado com êxito. Os clientes podem montar o volume usando o caminho de junção do volume FlexCache.

Informações relacionadas

"Peering de cluster e SVM"

FlexCache writeback

Visão geral do ONTAP FlexCache write-back

Introduzido no ONTAP 9.15,1, o FlexCache write-back é um modo alternativo de operação para escrever em um cache. Write-back permite que a gravação seja comprometida com o armazenamento estável no cache e reconhecida ao cliente sem esperar que os dados cheguem à origem. Os dados são escoados assincronamente de volta à origem. Como resultado, um sistema de arquivos distribuído globalmente permite que as gravações sejam executadas em velocidades quase locais para workloads e ambientes específicos, oferecendo benefícios significativos de performance.

O ONTAP 9.12,1 introduziu um recurso de write-back como uma prévia pública. Isto é referido como versão de write-back 1 (wbv1) e não deve ser pensado como o mesmo que write-back no ONTAP 9.15,1, que é referido como versão de write-back 2 (wbv2).

Write-back vs write-around

Desde que o FlexCache foi introduzido no ONTAP 9.5, ele tem sido um cache gravável de leitura; no entanto, ele operou no modo write-around. As gravações no cache foram enviadas para a origem para serem comprometidas com o armazenamento estável. Após a origem ter comprometido com sucesso a gravação para armazenamento estável, ele reconheceu a gravação no cache. O cache então reconheceria a gravação para o cliente. Isso fez com que cada gravação incorresse a penalidade de atravessar a rede entre o cache e a origem. O FlexCache write-back muda isso.

Depois de atualizar para o ONTAP 9.15,1, você pode converter um cache tradicional write-around para um cache write-back e, se necessário, voltar para write-around. Isso pode, no entanto, tornar a leitura de logs de diagnóstico mais difícil caso surja um problema.

	Escrever em torno	Write-back
Versão de ONTAP	Mais de 9,6 anos	Mais de 9.15.1 anos
Caso de uso	Carga de trabalho com leitura intensa	Carga de trabalho com gravação intensa
Dados comprometidos em	Origem	Cache
Experiência do cliente	Tipo WAN	LAN-lke
Limites	100 por origem	10 por origem
"CAP Theorem"	Disponível e tolerante à partição	Disponível e consistente

Terminologia de reescrita do FlexCache

Entenda os principais conceitos e termos trabalhando com o FlexCache write-back.

Prazo	Definição
dados sujos	Dados que foram comprometidos com o armazenamento estável no cache, mas não foram lavados para a origem.
* Delegação exclusiva de bloqueio (XLD)*	Uma autoridade de bloqueio em nível de protocolo concedida em uma base por arquivo para um cache. Essa autoridade permite que o cache distribua bloqueios de gravação exclusivos aos clientes sem entrar em Contato com a origem.
Delegação de bloqueio compartilhado (SLD)	Uma autoridade de bloqueio em nível de protocolo concedida em uma base por arquivo para um cache. Essa autoridade permite que o cache distribua bloqueios de leitura compartilhados aos clientes sem entrar em Contato com a origem.
Resposta	Um modo de operação do FlexCache onde as gravações em um cache são comprometidas com o armazenamento estável nesse cache e imediatamente reconhecidas ao cliente. Os dados são assincronamente escritos de volta à origem.

Prazo	Definição
* Escreva-em torno*	Um modo de operação do FlexCache onde as gravações em um cache são encaminhadas para a origem para serem comprometidas com o armazenamento estável. Uma vez confirmada, a origem reconhecerá a gravação no cache, e o cache reconhecerá a gravação no cliente.
Sistema de Registro de dados sujos (DDRS)	Um mecanismo proprietário que mantém o controle dos dados sujos em um cache habilitado para write-back em uma base por arquivo.
Origem	Um FlexGroup ou FlexVol que contém os dados de origem para todos os volumes de cache FlexCache. Ele é a única fonte da verdade, orquestra o bloqueio e garante 100% de consistência, moeda e coerência dos dados.
Cache	Um FlexGroup que é um volume de cache esparso da origem do FlexCache.

Consistente, atual e coerente

O FlexCache é a solução da NetApp para ter os dados certos, em qualquer lugar e sempre. O FlexCache é 100% consistente, atual e coerente 100% do tempo:

- **Consistente:** os dados são os mesmos onde quer que sejam acessados.
- **Current:** os dados estão sempre atualizados.
- **Coerente:** os dados estão corretos/não corrompidos.

Diretrizes de reescrita do ONTAP FlexCache

O FlexCache write-back envolve muitas interações complexas entre a origem e caches. Para um desempenho ideal, você deve garantir que seu ambiente siga estas diretrizes. Estas diretrizes baseiam-se na versão principal mais recente do ONTAP (ONTAP 9.15.1.) disponível no momento da criação de conteúdo.

PRÁTICA recomendada: Teste sua carga de trabalho de produção em um ambiente não-produção. Isso é ainda mais importante se você estiver implementando o FlexCache write-back fora dessas diretrizes.

As seguintes diretrizes são bem testadas internamente na NetApp. É ***fortemente*** recomendado que você fique dentro deles. Se não o fizer, poderá ocorrer um comportamento inesperado.

- Melhorias significativas para o FlexCache write-back foram introduzidas no ONTAP 9.15.1P5. É ***fortemente*** aconselhado que você execute a versão recomendada atual após 9.15.1P5 nos clusters origem e cache.
- Em sua iteração atual, os caches write-back do FlexCache devem ser configurados com um único constituinte para todo o volume FlexCache. FlexCaches multiconstitutivos pode resultar em despejos indesejados de dados do cache.
- O teste foi executado para arquivos menores que 100GB e tempos de ida e volta da WAN entre o cache e a origem não superiores a 100ms. Quaisquer cargas de trabalho fora desses limites podem resultar em caraterísticas de desempenho inesperadas.
- A gravação em fluxos de dados alternativos SMB faz com que o arquivo principal seja despejado do cache. Todos os dados sujos para o arquivo principal precisam ser lavados para a origem antes que qualquer outra operação possa ocorrer nesse arquivo. O fluxo de dados alternativo também é

encaminhado para a origem.

- Renomear um arquivo faz com que o arquivo seja despejado do cache. Todos os dados sujos para o arquivo precisam ser lavados para a origem antes que qualquer outra operação possa ocorrer nesse arquivo.
- Neste momento, os únicos atributos que podem ser alterados ou definidos em um arquivo no volume FlexCache habilitado para gravação são:
  - Carimbos de data/hora
  - Bits de modo
  - ACLs do NT
  - Proprietário
  - Grupo
  - Tamanho

    Quaisquer outros atributos que sejam alterados ou definidos são encaminhados para o Origin, o que pode resultar na remoção do arquivo do cache. Se você precisar que outros atributos sejam alterados ou definidos no cache, peça à equipe da sua conta para abrir um PVR.
- Os instantâneos tirados na origem causam a recuperação de todos os dados sujos pendentes de cada cache habilitado para gravação associada a esse volume de origem. Isso pode exigir várias tentativas da operação se houver uma atividade significativa de retorno de gravação em andamento, já que os despejos desses arquivos sujos podem levar algum tempo.
- A origem deve permanecer abaixo de 80% cheio. Os volumes de cache não recebem delegações de bloqueio exclusivo se não houver pelo menos 20% de espaço restante no volume de origem. As chamadas para um cache habilitado para write-back são encaminhadas para a origem nesta situação. Isso ajuda a evitar a falta de espaço na origem, o que resultaria em deixar dados sujos órfãos em um cache habilitado para write-back.

Arquitetura de back-back do ONTAP FlexCache

O FlexCache foi projetado com forte consistência em mente, incluindo ambos os modos de operação de gravação: Write-back e write-around. Tanto o modo de operação tradicional write-around quanto o novo modo de operação write-back introduzido no ONTAP 9.15,1 garantem que os dados acessados serão sempre 100% consistentes, atuais e coerentes.

Os conceitos a seguir detalham como o FlexCache write-back funciona.

Delegações

As delegações de bloqueio e de dados ajudam a FlexCache a manter os dados de cache de gravação e gravação consistentes, coerentes e atuais. A origem orquestra ambas as delegações.

Bloquear delegações

Uma delegação de bloqueio é uma autoridade de bloqueio em nível de protocolo que a origem concede a um cache por ficheiro para emitir bloqueios de protocolo aos clientes, conforme necessário. Estes incluem Delegações exclusivas de bloqueio (XLD) e Delegações de bloqueio partilhado (SLD).

XLD e write-back

Para garantir que o ONTAP nunca tenha que reconciliar uma gravação conflitante, um XLD é concedido a um cache onde um cliente solicita gravar em um arquivo. É importante ressaltar que apenas um XLD pode existir para qualquer arquivo a qualquer momento, o que significa que nunca haverá mais de um escritor para um arquivo de cada vez.

Quando a solicitação para gravar em um arquivo entra em um cache habilitado para write-back, as seguintes etapas ocorrem:

1. O cache verifica se ele já tem um XLD para o arquivo solicitado. Em caso afirmativo, ele concederá o bloqueio de gravação ao cliente, desde que outro cliente não esteja escrevendo para o arquivo no cache. Se o cache não tiver um XLD para o arquivo solicitado, ele solicitará um da origem. Esta é uma chamada proprietária que atravessa a rede entre clusters.
2. Ao receber a solicitação XLD do cache, a origem verificará se há um XLD pendente para o arquivo em outro cache. Se assim for, ele irá lembrar o XLD desse arquivo, que aciona um flush de qualquer um dados sujosdesse cache de volta para a origem.
3. Uma vez que os dados sujos desse cache são lavados de volta e comprometidos com armazenamento estável na origem, a origem concederá o XLD para o arquivo ao cache solicitante.
4. Uma vez que o XLD do arquivo é recebido, o cache concede o bloqueio ao cliente, e a gravação começa.

Um diagrama de sequência de alto nível que abrange alguns destes passos é abordado no [write-back-sequence-diagram]diagrama de sequência.

Do ponto de vista do cliente, todo o bloqueio funcionará como se estivesse escrevendo para um FlexVol padrão ou FlexGroup com um pequeno atraso potencial quando o bloqueio de gravação é solicitado.

Em sua iteração atual, se um cache habilitado para write-back contiver o XLD para um arquivo, o ONTAP bloqueará **qualquer** acesso a esse arquivo em outros caches, incluindo `READ` operações.

> Há um limite de 170 XLDs por componente de origem.

Delegações de dados

Uma delegação de dados é uma garantia por arquivo dada a um cache pela origem em que os dados armazenados em cache para esse arquivo estão atualizados. Desde que o cache tenha uma delegação de dados para um arquivo, ele pode servir os dados em cache para esse arquivo ao cliente sem ter que entrar em Contato com a origem. Se o cache não tiver uma delegação de dados para o arquivo, ele deve entrar em Contato com a origem para receber os dados solicitados pelo cliente.

No modo write-back, a delegação de dados de um arquivo é revogada se um XLD for levado para esse arquivo em outro cache ou na origem. Isso efetivamente bloqueia o arquivo dos clientes em todos os outros caches e a origem, mesmo para leituras. Este é um trade off que deve ser feito para garantir que os dados antigos nunca sejam acessados.

As leituras em um cache habilitado para write-back geralmente funcionam como leituras em um cache write-around. Em caches habilitados para write-around e write-back, pode haver um acerto inicial `READ` no desempenho quando o arquivo solicitado tiver um bloqueio de gravação exclusivo em um cache habilitado para write-back que não seja onde a leitura é emitida. O XLD tem de ser revogado e os dados sujos têm de ser comprometidos com a origem antes de a leitura no outro cache poder ser assistida.

Rastrear dados sujos

Write-back do cache para o Origin acontece assincronamente. Isso significa que os dados sujos não são imediatamente gravados de volta à origem. O ONTAP emprega um sistema de Registro de dados sujos para

manter o controle dos dados sujos por arquivo. Cada Registro de dados sujos (DDR) representa aproximadamente 20MBMB de dados sujos para um arquivo específico. Quando um arquivo está sendo escrito ativamente, o ONTAP começará a liberar dados sujos de volta depois que dois DDRS foram preenchidos e o terceiro DDR está sendo escrito. Isso resulta em aproximadamente 40MBMB de dados sujos restantes em um cache durante as gravações. Para protocolos stateful (NFSv4.x, SMB), os 40MB restantes de dados serão lavados de volta para a origem quando o arquivo for fechado. Para protocolos sem estado (NFSv3), o 40MB de dados será limpo de volta quando o acesso ao arquivo for solicitado em um cache diferente ou depois que o arquivo estiver ocioso por dois ou mais minutos, até um máximo de cinco minutos. Para obter mais informações sobre a lavagem de dados sujos acionada por temporizador ou acionada por espaço, Limpadores de cacheconsulte .

Além dos DDRS e depuradores, algumas operações nas front-end também acionam a descarga de todos os dados sujos de um arquivo:

- `SETATTR`
  - "Os SETATTR que modificam apenas mtime, atime e/ou ctime podem ser processados no cache, evitando a penalidade da WAN.
- `CLOSE`
- `OPEN` em outro cache
- `READ` em outro cache
- `READDIR` em outro cache
- `READDIRPLUS` em outro cache
- `WRITE` em outro cache

Modo desligado

Quando um XLD para um arquivo é mantido em um cache write-around e esse cache é desconetado da origem, as leituras para esse arquivo ainda são permitidas nos outros caches e origem. Esse comportamento difere quando um XLD é mantido por um cache habilitado para write-back. Neste caso, se o cache estiver desconetado, as leituras para o arquivo ficarão em todos os lugares. Isso ajuda a garantir que 100% de consistência, moeda e coerência sejam mantidas. As leituras são permitidas no modo write-around porque a origem é garantida para ter todos os dados disponíveis que foram gravados-reconhecidos para o cliente. No modo write-back durante uma desconexão, a origem não pode garantir que todos os dados gravados e reconhecidos pelo cache habilitado para write-back chegaram à origem antes da desconexão ocorrer.

No caso de um cache com um XLD para um arquivo ser desconetado por um longo período de tempo, um administrador do sistema pode revogar manualmente o XLD na origem. Isso permitirá que o IO para o arquivo seja retomado nos caches sobreviventes e na origem.

Revogar manualmente o XLD resultará na perda de quaisquer dados sujos para o arquivo no cache desconetado. A revogação manual de um XLD só deve ser feita no caso de uma interrupção catastrófica entre o cache e a origem.

Limpadores de cache

Existem depuradores no ONTAP que são executados em resposta a eventos específicos, como expiração de um temporizador ou limites de espaço sendo violados. Os limpadores pegam um bloqueio exclusivo no arquivo que está sendo limpo, efetivamente congelando io para esse arquivo até que a limpeza seja concluída.

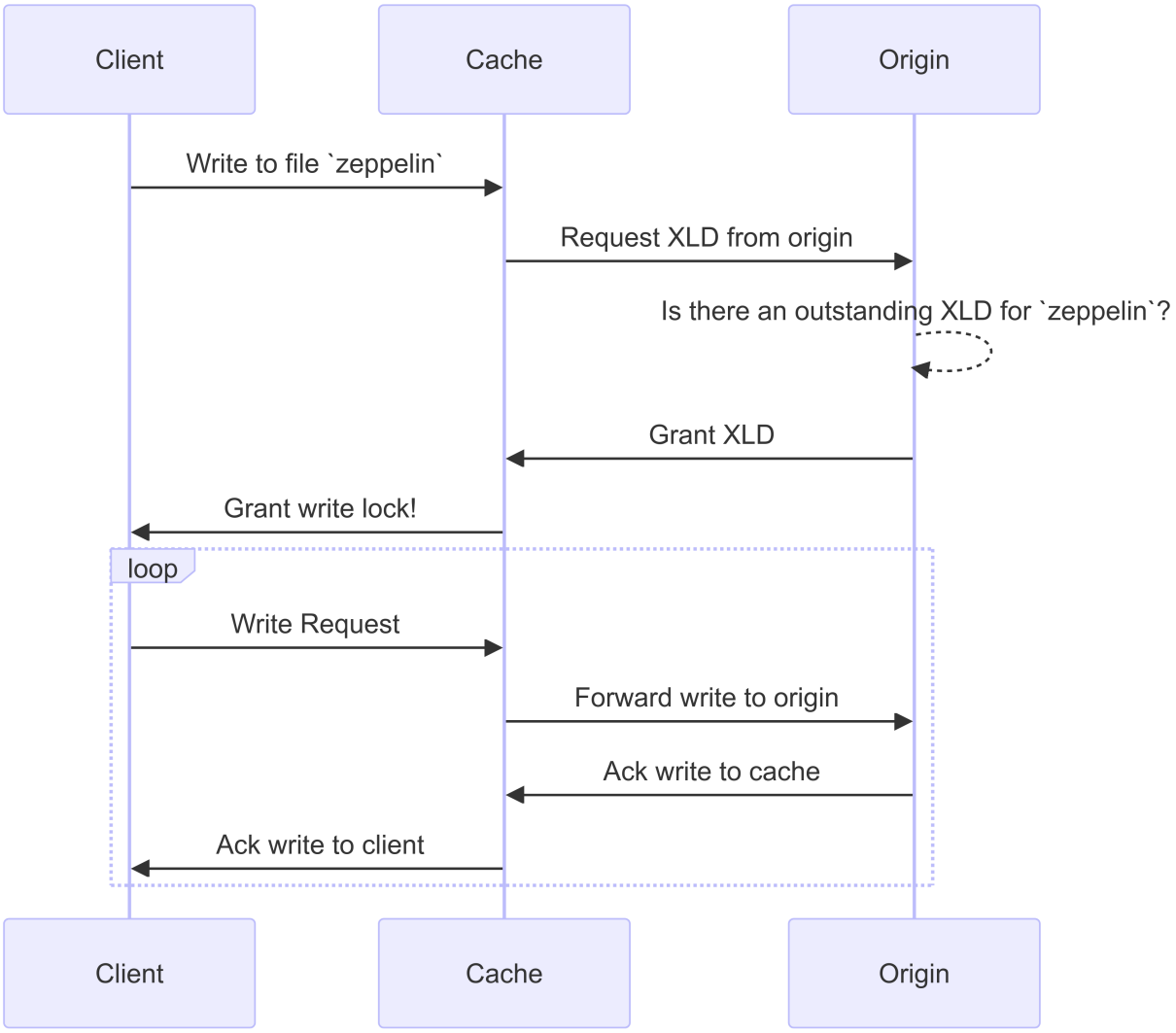
Os lavadores incluem:

- **Mtime-based scrubber no cache:** este scrubber começa a cada cinco minutos e scrubs qualquer arquivo não modificado por dois minutos. Se algum dado sujo para o arquivo ainda estiver no cache, o IO para esse arquivo será desativado e o write-back será acionado. O IO será retomado após a conclusão do write-back.
- **Mtime-based scrubber on Origin:** muito parecido com o scrubber baseado em mtime no cache, isso também é executado a cada cinco minutos. No entanto, ele analisa qualquer arquivo não modificado por 15 minutos, lembrando a delegação do inode. Este depurador não inicia qualquer write-back.
- **RW limit-based scrubber on Origin:** o ONTAP monitora quantas delegações de bloqueio RW são distribuídas por componente de origem. Se este número ultrapassar 170, o ONTAP começa a analisar as delegações de bloqueio de escrita numa base de utilização menos recente (LRU).
- **Scrubber baseado no espaço no cache:** se um volume de FlexCache atingir 90% cheio, o cache é limpo, despejando em uma base LRU.
- **Scrubber baseado no espaço sobre a origem:** se um volume de origem FlexCache atingir 90% cheio, o cache é limpo, despejando em uma base LRU.

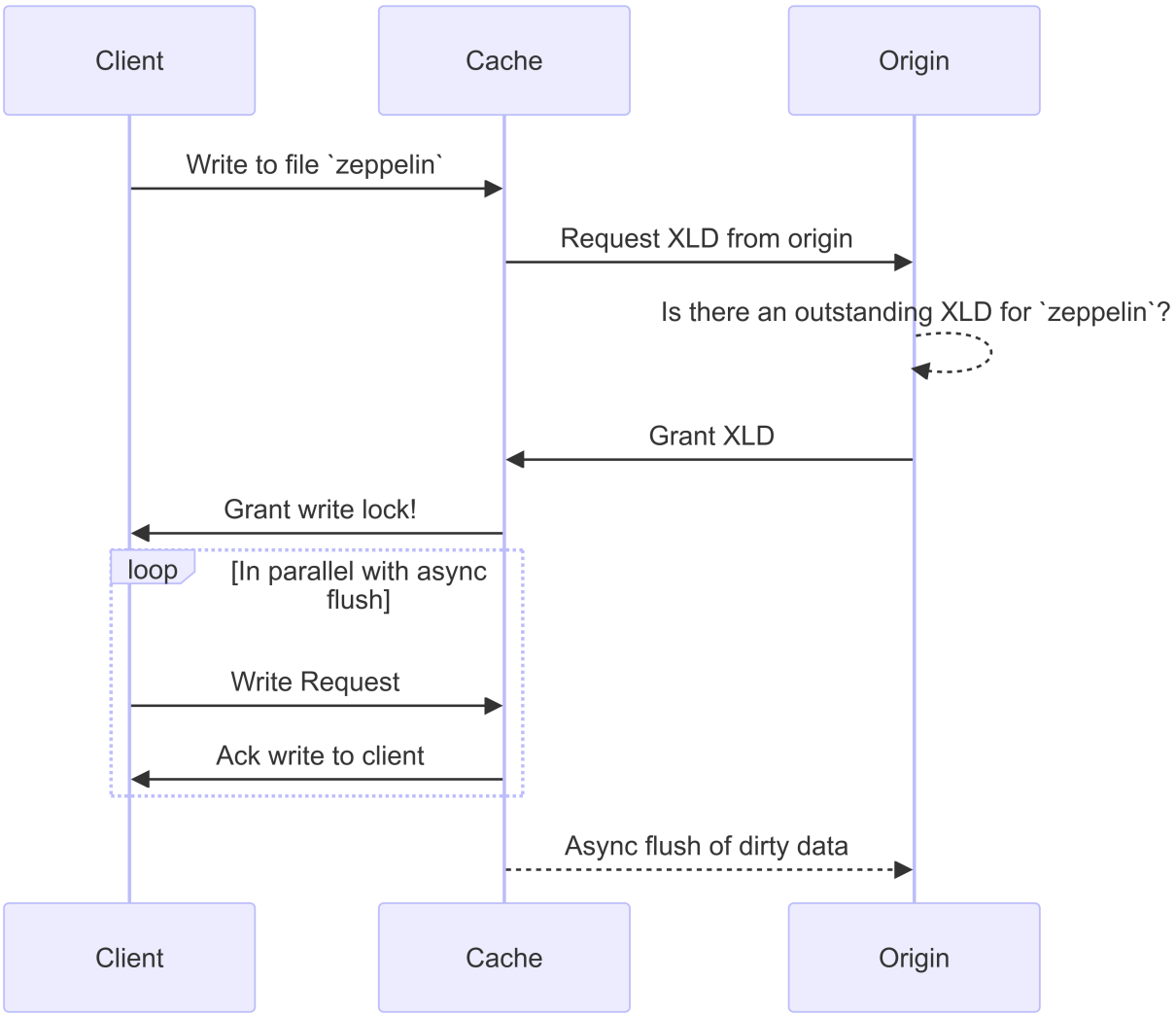
Diagramas de sequência

Esses diagramas de sequência descrevem a diferença nos reconhecimentos de escrita entre o modo write-around e write-back.

Escrever em torno


Client
Cache
Origin
Write to file `zeppelin`
Request XLD from origin
Is there an outstanding XLD for `zeppelin`?
Grant XLD
Grant write lock!
loop
Write Request
Forward write to origin
Ack write to cache
Ack write to client
Client
Cache
Origin

Write-back



Casos de uso de retorno de gravação do ONTAP FlexCache

Estes são os perfis de escrita mais adequados para um FlexCache habilitado para gravação. Você deve testar seu workload para ver se o back-back ou a gravação fornecem a melhor performance.

Write-back não é um substituto para write-around. Embora o write-back seja projetado com workloads com muita gravação, o write-around ainda é a melhor opção para muitos workloads.

Workloads de destino

Tamanho do ficheiro

O tamanho do arquivo é menos importante do que o número de gravações emitidas entre o `OPEN` e `CLOSE` chamadas para um arquivo. Arquivos pequenos têm, inerentemente, `WRITE` menos chamadas, tornando-os menos ideais para write-back. Arquivos grandes podem ter mais gravações entre `OPEN` e `CLOSE` chamadas, mas isso não é garantido.

Consulte "Diretrizes de reescrita do FlexCache"a página para obter as recomendações mais recentes sobre o tamanho máximo do arquivo.

Tamanho da gravação

Ao gravar de um cliente, outras chamadas nas modificadas são envolvidas além de chamadas de gravação. Estes incluem, mas não estão limitados a:

- `CREATE`
- `OPEN`
- `CLOSE`
- `SETATTR`
- `SET_INFO`

`SETATTR` e `SET_INFO` as chamadas que definem `mtime`, `atime`, , `ctime` `owner` , `group` ou `size` são processadas no cache. O resto dessas chamadas deve ser processado na origem e acionar uma gravação de qualquer dado sujo acumulado no cache habilitado para write-back para o arquivo que está sendo operado. O IO para o arquivo será silenciado até que o write-back esteja concluído.

Saber que essas chamadas devem atravessar a WAN ajuda você a identificar cargas de trabalho adequadas para back-back. Geralmente, quanto mais gravações que podem ser feitas entre `OPEN` e `CLOSE` chamadas sem que uma das outras chamadas listadas acima seja emitida, melhor será o ganho de desempenho de retorno de gravação.

Leitura-após-escrita

As cargas de trabalho de leitura após gravação têm tido um desempenho insatisfatório na FlexCache. Isto deve-se ao modo de operação de escrita antes de 9.15.1. A `WRITE` chamada para o arquivo tem que ser confirmada na origem, e a chamada subsequente `READ` teria que puxar os dados de volta para o cache. Isso resulta em ambas as operações que incorrem na penalidade da WAN. Portanto, as cargas de trabalho de leitura após gravação são desencorajadas para o FlexCache no modo write-around. Com a introdução do write-back em 9.15.1, os dados agora são comprometidos no cache e podem ser lidos imediatamente a partir do cache, eliminando a penalidade da WAN. Se o seu workload incluir leitura após gravação em volumes FlexCache, você deverá configurar o cache para operar no modo write-back.

Se a leitura após a gravação for uma parte crítica da sua carga de trabalho, você deve configurar o cache para operar no modo write-back.

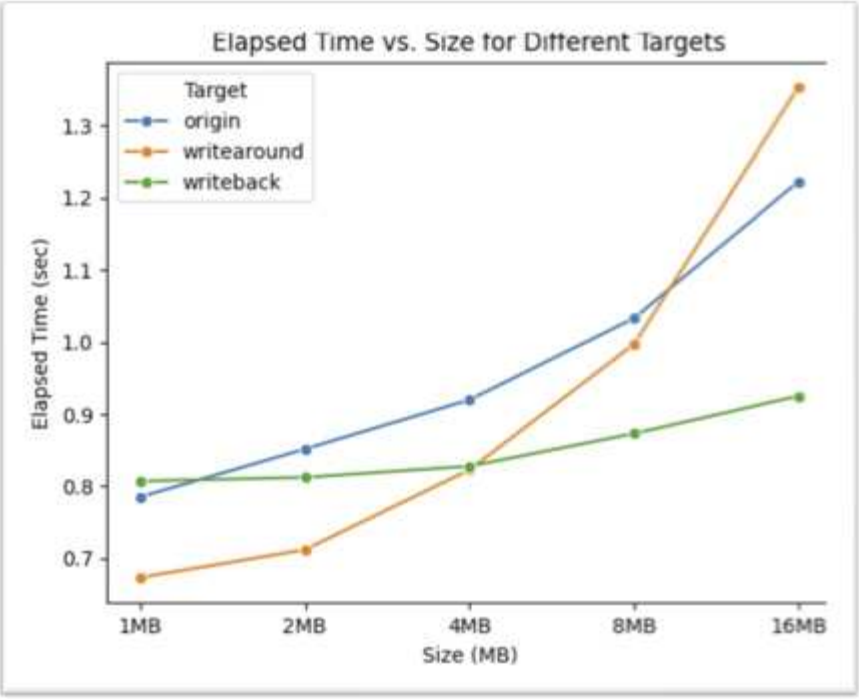
Escrever-após-escrever

Quando um arquivo acumula dados sujos em um cache, o cache grava os dados de volta para a origem de forma assíncrona. Isso naturalmente leva a momentos em que o cliente fecha o arquivo com dados sujos ainda esperando para ser lavado de volta à origem. Se outro arquivo aberto ou escrito aparecer para o arquivo que foi fechado e ainda tem dados sujos, a gravação será suspensa até que todos os dados sujos tenham sido lavados para origem.

Considerações sobre latência

Quando o FlexCache opera no modo write-back, torna-se mais benéfico para os clientes nas à medida que a latência aumenta. No entanto, há um ponto em que a sobrecarga do write-back supera as vantagens obtidas em ambientes de baixa latência. Em alguns testes do NetApp, os benefícios de write-back começaram em torno de uma latência mínima entre cache e origem do 8ms. Essa latência varia de acordo com o workload, portanto, teste para saber o ponto de retorno do workload.

O gráfico a seguir mostra o ponto de retorno para write-back em testes de laboratório do NetApp. O `x` eixo é o tamanho do arquivo e o `y` eixo é o tempo decorrido. O teste utilizou NFSv3, montagem com um `rsize` e `wsize` de 256KB e 64ms de latência WAN. Este teste foi realizado usando uma pequena instância do ONTAP Select para o cache e origem, e uma única operação de escrita em thread. Seus resultados podem variar.



O write-back não deve ser usado para armazenamento em cache sem brilho. O armazenamento em cache do Intracluster ocorre quando a origem e o cache estão no mesmo cluster.

Pré-requisitos de reescrita do ONTAP FlexCache

Antes de implantar o FlexCache no modo write-back, verifique se você atendeu a esses requisitos de desempenho, software, licenciamento e configuração do sistema.

CPU e memória

Cada nó do cluster de origem deve ter pelo menos 128GB GB de RAM e 20 CPUs para absorver as mensagens de retorno iniciadas por caches habilitados para write-back. Este é o equivalente a um A400 ou superior. Se o cluster de origem servir como origem para múltiplas FlexCaches habilitadas para write-back, ele exigirá mais CPU e RAM.

Usar uma origem subdimensionada para sua carga de trabalho pode ter impactos profundos no desempenho no cache habilitado para gravação ou na origem.

Versão de ONTAP

- A origem ***must*** está executando o ONTAP 9.15,1 ou posterior.
- Qualquer cluster de cache que precise operar no modo write-back ***must*** esteja executando o ONTAP 9.15,1 ou posterior.
- Qualquer cluster de cache que não precise operar no modo write-back pode executar qualquer versão do ONTAP geralmente suportada.

Licenciamento

O FlexCache, incluindo o modo de operação write-back, está incluído na compra do ONTAP. Nenhuma licença

extra é necessária.

Peering

- Os clusters de origem e cache devem ser "cluster com peered"
- As máquinas virtuais de servidor (SVMs) no cluster de origem e cache devem estar "svm peered" com a opção FlexCache.

> Você não precisa fazer um peer de cluster de cache para outro cluster de cache. Também não há necessidade de fazer um cache SVM para outro cache SVM.

Interoperabilidade com ONTAP FlexCache Write-back

Entenda essas considerações de interoperabilidade ao implantar o FlexCache no modo write-back.

Versão de ONTAP

Para usar o modo de operação write-back, tanto o cache quanto o Origin **devem** estar executando o ONTAP 9.15,1 ou posterior.

> Os clusters em que um cache habilitado para write-back é desnecessário podem executar versões anteriores do ONTAP, mas esse cluster só pode operar no modo write-around.

Você pode ter uma combinação de versões do ONTAP em seu ambiente.

Cluster	Versão de ONTAP	Write-back suportado?
Origem	ONTAP 9.15,1	N/A †
Cluster 1	ONTAP 9.15,1	Sim
Cluster 2	ONTAP 9.14,1	Não

Cluster	Versão de ONTAP	Write-back suportado?
Origem	ONTAP 9.14,1	N/A †
Cluster 1	ONTAP 9.15,1	Não
Cluster 2	ONTAP 9.15,1	Não

† *Origins não são um cache, então nem o suporte de write-back nem write-around é aplicável.*

> No [example2-table], nenhum dos clusters pode ativar o modo write-back porque a origem não está executando o ONTAP 9.15,1 ou posterior, o que é um requisito estrito.

Interoperabilidade do cliente

Qualquer cliente geralmente suportado pelo ONTAP pode acessar um volume FlexCache, independentemente de estar operando no modo write-around ou write-back. Para obter uma lista atualizada dos clientes suportados, consulte NetApp's "matriz de interoperabilidade".

Embora a versão do cliente não importa especificamente, o cliente deve ser novo o suficiente para suportar

NFSv3, NFSv4,0, NFSv4,1, SMB2.x ou SMB3.x. SMB1 e NFSv2 são protocolos obsoletos e não são suportados.

Escreva-back e escreva-around

Como visto [example1-table]no , o FlexCache operando no modo write-back pode coexistir com caches operando no modo write-around. É aconselhável comparar write-around com write-back com sua carga de trabalho específica.

Se a performance de um workload for a mesma entre write-back e write-around, use write-around.

Interoperabilidade do recurso ONTAP

Para obter a lista mais atualizada de interoperabilidade de recursos do FlexCache, "Os recursos suportados e não suportados para volumes FlexCache"consulte .

Ative e gerencie o ONTAP FlexCache write-back

A partir do ONTAP 9.15,1, é possível ativar o modo de gravação FlexCache em volumes FlexCache para fornecer melhor desempenho para ambientes de computação de borda e caches com cargas de trabalho com gravação intensa. Você também pode determinar se o write-back está habilitado em um volume FlexCache ou desativar o write-back no volume quando necessário.

Quando o write-back está ativado no volume do cache, as solicitações de gravação são enviadas para o cache local em vez do volume de origem.

Antes de começar

Tem de estar no modo de privilégio avançado.

Crie um novo volume FlexCache com a opção write-back ativada

Passos

Você pode criar um novo volume FlexCache com a opção de gravação ativada usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

1. Se o volume FlexCache estiver em um cluster diferente do volume de origem, crie uma relação de par de cluster:
   a. No cluster local, clique em **proteção > Visão geral**.
   b. Expanda **Intercluster Settings**, clique em **Add Network interfaces** e adicione interfaces entre clusters ao cluster.

      Repita este procedimento no painel remoto.

   c. No cluster remoto, clique em **proteção > Visão geral**. Clique na seção Cluster Peers e clique em **Generate Passphrase**.
   d. Copie a frase-passe gerada e cole-a no cluster local.
   e. No cluster local, em Cluster Peers, clique em **Peer clusters** e emparelhe os clusters locais e remotos.
2. Se o volume FlexCache estiver em um cluster diferente do volume de origem, crie um relacionamento de pares SVM:

   Em **Storage VM Peers**, clique em e em **Peer Storage VMs** para fazer o peer nas VMs de armazenamento.

   Se o volume FlexCache estiver no mesmo cluster, não será possível criar um relacionamento de pares SVM usando o System Manager.
3. Selecione **armazenamento > volumes**.
4. Selecione **Adicionar**.
5. Selecione **mais Opções** e, em seguida, selecione **Adicionar como cache para um volume remoto**.
6. Selecione **Enable FlexCache write-back**.

CLI

1. Se o volume FlexCache a ser criado estiver em um cluster diferente, crie uma relação de par de cluster:
   a. No cluster de destino, crie uma relação de mesmo nível com o cluster de origem de proteção de dados:

      ```
      cluster peer create -generate-passphrase -offer-expiration
      MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
      <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
      -ipspace <ipspace_name>
      ```

      A partir do ONTAP 9.6, a criptografia TLS é ativada por padrão ao criar uma relação de par de cluster. A criptografia TLS é suportada para a comunicação entre clusters entre os volumes de origem e FlexCache. Você também pode desativar a criptografia TLS para o relacionamento de pares de cluster, se necessário.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

a. No cluster de origem, autentique o cluster de origem no cluster de destino:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. Se o volume FlexCache estiver em um SVM diferente daquele do volume de origem, crie um relacionamento de mesmo nível com `flexcache` o como aplicação:

a. Se o SVM estiver em um cluster diferente, crie uma permissão SVM para os SVMs de peering:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

O exemplo a seguir ilustra como criar uma permissão SVM peer que se aplica a todos os SVMs locais:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. Crie o relacionamento entre pares SVM:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Criar um volume FlexCache com write-back habilitado:

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

Ative o FlexCache write-back em um volume FlexCache existente

Você pode habilitar a gravação do FlexCache em um volume FlexCache existente usando o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

System Manager

1. Selecione **armazenamento > volumes** e selecione um volume FlexCache existente.
2. Na página Visão geral do volume, clique em **Editar** no canto superior direito.
3. Na janela **Editar volume**, selecione **Enable FlexCache write-back**.

CLI

1. Ativar o write-back em um volume FlexCache existente:

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

Verifique se o FlexCache write-back está ativado

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para determinar se o retorno de gravação do FlexCache está habilitado.

System Manager

1. Selecione **armazenamento > volumes** e selecione um volume.
2. No volume **Visão geral**, localize **Detalhes do FlexCache** e verifique se o FlexCache write-back está definido como **Enabled** no volume do FlexCache.

CLI

1. Verifique se o FlexCache write-back está ativado:

```
volume flexcache config show -volume <cache_flexgroup_name> -fields
is-writeback-enabled
```

Desative a opção write-back em um volume FlexCache

Antes de poder eliminar um volume FlexCache, tem de desativar o FlexCache write-back.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para desativar o retorno de gravação do FlexCache.

System Manager

1. Selecione **armazenamento > volumes** e selecione um volume FlexCache existente que tenha o FlexCache write-back habilitado.
2. Na página Visão geral do volume, clique em **Editar** no canto superior direito.
3. Na janela **Editar volume**, desmarque **Ativar retorno de gravação do FlexCache**.

CLI

1. Desativar write-back:

```
volume flexcache config modify -volume <cache_vol_name> -is
-writeback-enabled false
```

Perguntas frequentes sobre o ONTAP FlexCache write-back

Este FAQ pode ajudar se você está procurando uma resposta rápida para uma pergunta.

Eu quero usar write-back. Qual versão do ONTAP eu preciso para executar?

Tanto o cache quanto a origem devem estar executando o ONTAP 9.15.1 ou posterior. É recomendado

fortemente que você execute a versão P mais recente. A engenharia está constantemente melhorando o desempenho e a funcionalidade de caches habilitados para write-back.

Os clientes que acessam a origem podem ter um efeito sobre os clientes que acessam o cache habilitado para write-back?

Sim. A origem tem igual direito aos dados como qualquer um dos caches. Se uma operação for executada em um arquivo que exija que o arquivo seja despejado do cache ou uma delegação de bloqueio/dados seja revogada, o cliente no cache pode ver um atraso acessando o arquivo.

Posso aplicar QoS a FlexCaches habilitadas para gravação?

Sim. Cada cache e a origem podem ter políticas de QoS independentes aplicadas. Isso não terá efeito direto em qualquer tráfego iniciado de back-back entre clusters. Indiretamente, você pode reduzir o tráfego de retorno de gravação entre clusters limitando o tráfego front-end no cache habilitado para write-back.

O nas multiprotocolo é suportado em FlexCaches habilitados para write-back?

Sim. Multi-protocolo é totalmente suportado em FlexCaches com write-back habilitado. Atualmente, NFSv4,2 e S3 não são suportados pelo FlexCache operando no modo write-around ou write-back.

Os fluxos de dados alternativos SMB são compatíveis com FlexCaches habilitados para gravação?

Fluxos de dados alternativos (ANÚNCIOS) SMB são compatíveis, mas não são acelerados com o write-back. A gravação para os ANÚNCIOS é encaminhada para a origem, incorrendo na penalidade da latência da WAN. A gravação também expulsa o arquivo principal do qual OS ANÚNCIOS fazem parte do cache.

Posso alternar um cache entre o modo write-around e write-back depois que ele é criado?

Sim. Tudo o que você precisa fazer é alternar a `is-writeback-enabled` bandeira no `flexcache modify` command.

Gerenciar o FlexCache volumes

Considerações para auditoria de volumes do FlexCache

A partir do ONTAP 9.7, você pode auditar eventos de acesso a arquivos NFS em relacionamentos do FlexCache usando auditoria nativa do ONTAP e gerenciamento de políticas de arquivos com o FPolicy.

A partir do ONTAP 9.14,1, o FPolicy é compatível com volumes FlexCache com NFS ou SMB. Anteriormente, FPolicy não era compatível com volumes FlexCache com SMB.

Auditoria nativa e FPolicy são configurados e gerenciados com os mesmos comandos de CLI usados para volumes FlexVol. No entanto, há algum comportamento diferente com os volumes FlexCache.

- * Auditoria nativa*
  - Não é possível usar um volume FlexCache como destino para logs de auditoria.
  - Para auditar a leitura e a gravação em volumes do FlexCache, configure a auditoria tanto na SVM do cache quanto na SVM de origem.

    Isso ocorre porque as operações do sistema de arquivos são auditadas onde são processadas. Ou seja, as leituras são auditadas no SVM do cache e as gravações são auditadas no SVM de origem.

  - Para rastrear a origem das operações de gravação, o UUID SVM e o MSID são anexados no log de auditoria para identificar o volume FlexCache a partir do qual a gravação se originou.

- Embora as listas de controle de acesso do sistema (SACLs) possam ser definidas em um arquivo usando protocolos NFSv4 ou SMB, os volumes FlexCache suportam apenas NFSv3. Portanto, os SACLs só podem ser definidos no volume de origem.

- **FPolicy**
  - Embora as gravações em um volume FlexCache sejam confirmadas no volume de origem, as configurações do FPolicy monitoram as gravações no volume de cache. Isso é diferente da auditoria nativa, na qual as gravações são auditadas no volume de origem.
  - Embora o ONTAP não exija a mesma configuração de FPolicy nos SVMs de cache e origem, é recomendável que você implante duas configurações semelhantes. Você pode fazer isso criando uma nova política de FPolicy para o cache, configurada como a SVM de origem, mas com o escopo da nova política limitada ao cache SVM.

Sincronizar propriedades de um volume FlexCache de um volume de origem

Algumas das propriedades de volume do volume FlexCache devem ser sempre sincronizadas com as do volume de origem. Se as propriedades de volume de um volume FlexCache não forem sincronizadas automaticamente depois que as propriedades forem modificadas no volume de origem, será possível sincronizar manualmente as propriedades.

Sobre esta tarefa

As seguintes propriedades de volume de um volume FlexCache devem ser sempre sincronizadas com as do volume de origem:

- Estilo de (`-security-style`segurança)
- Nome do volume (`-volume-name`)
- Tamanho máximo do diretório (`-maxdir-size`)
- Leitura mínima (`-min-readahead`antecipada)

Passo

1. No volume FlexCache, sincronize as propriedades do volume:

   ```
   volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
   ```

   ```
   cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
   ```

Atualize as configurações de uma relação do FlexCache

Após eventos como movimentação de volume, realocação de agregados ou failover de storage, as informações de configuração de volume no volume de origem e no volume FlexCache serão atualizadas automaticamente. Caso as atualizações automáticas falhem, uma mensagem EMS é gerada e, em seguida, você deve atualizar manualmente a configuração para a relação FlexCache.

Se o volume de origem e o volume FlexCache estiverem no modo desconetado, talvez seja necessário executar algumas operações adicionais para atualizar um relacionamento FlexCache manualmente.

Sobre esta tarefa

Se você quiser atualizar as configurações de um volume FlexCache, você deve executar o comando a partir do volume de origem. Se você quiser atualizar as configurações de um volume de origem, você deve executar o comando a partir do volume FlexCache.

Passo

1. Atualize a configuração da relação FlexCache:

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

Ativar atualizações de tempo de acesso ao ficheiro

A partir do ONTAP 9.11,1, é possível ativar o `-atime-update` campo no volume FlexCache para permitir atualizações de tempo de acesso ao arquivo. Você também pode definir um período de atualização de tempo de acesso com o `-atime-update -period` atributo. O `-atime-update-period` atributo controla a frequência com que atualizações de tempo de acesso podem ocorrer e quando elas podem se propagar para o volume de origem.

Visão geral

O ONTAP fornece um campo de nível de volume chamado `-atime-update`, para gerenciar atualizações de tempo de acesso em arquivos e diretórios que são lidos usando LEITURA, READLINK e READDIR. Atime é usado para decisões de ciclo de vida de dados para arquivos e diretórios que são acessados com pouca frequência. Os arquivos acessados com pouca frequência são eventualmente migrados para o armazenamento de arquivos e, muitas vezes, são movidos mais tarde para fita.

O campo atime-update é desativado por padrão em volumes FlexCache existentes e recém-criados. Se você estiver usando o FlexCache volumes com versões do ONTAP anteriores a 9.11.1, você deve deixar o campo atime-update desativado para que os caches não sejam desnecessariamente despejados quando uma operação de leitura for executada no volume de origem. No entanto, com grandes caches do FlexCache, os administradores usam ferramentas especiais para gerenciar dados e ajudar a garantir que os dados ativos permaneçam no cache e que os dados inativos sejam purgados. Isto não é possível quando a atualização de tempo está desativada. No entanto, a partir do ONTAP 9.11,1, você pode ativar `-atime-update` e `-atime -update-period`, usar as ferramentas necessárias para gerenciar os dados em cache.

Antes de começar

Todos os volumes do FlexCache devem estar executando o ONTAP 9.11,1 ou posterior.

Sobre esta tarefa

A configuração `-atime-update-period` para 86400 segundos não permite mais de uma atualização de tempo de acesso por período de 24 horas, independentemente do número de operações semelhantes a leitura realizadas em um arquivo.

Definir `-atime-update-period` como 0 envia mensagens para a origem para cada acesso de leitura. A origem então informa cada volume de FlexCache que o tempo está desatualizado, o que afeta o desempenho.

Passos

1. Ative as atualizações de tempo de acesso aos ficheiros e defina a frequência de atualização:

   `volume modify -volume vol_name -vserver SVM_name -atime-update true -atime -update-period seconds`

   O exemplo a seguir ativa `-atime-update` e define `-atime-update-period` para 86400 segundos ou 24 horas:

   ```
   c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime
   -update-period 86400
   ```

2. Verifique se `-atime-update` está ativado:

   `volume show -volume vol_name -fields atime-update,atime-update-period`

   ```
   c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-
   update-period
   vserver volume         atime-update atime-update-period
   ------- -------------- ------------ -------------------
   vs2_c1  cache1_origin1 true         86400
   ```

Ative o bloqueio global de ficheiros

A partir do ONTAP 9.10,1, o bloqueio global de arquivos pode ser aplicado para evitar leituras em todos os arquivos armazenados em cache relacionados.

Com o bloqueio global de arquivos ativado, as modificações no volume de origem são suspensas até que todos os volumes do FlexCache estejam online. Você só deve ativar o bloqueio global de arquivos quando tiver controle sobre a confiabilidade das conexões entre cache e origem devido à suspensão e possíveis tempos limite de modificações quando os volumes FlexCache estiverem offline.

Antes de começar

- O bloqueio global de arquivos requer que os clusters que contêm a origem e todos os caches associados estejam executando o ONTAP 9.9,1 ou posterior. O bloqueio global de arquivos pode ser ativado em volumes FlexCache novos ou existentes. O comando pode ser executado em um volume e se aplica a todos os volumes FlexCache associados.
- Tem de estar no nível de privilégio avançado para ativar o bloqueio global de ficheiros.
- Se você reverter para uma versão do ONTAP anterior à 9,9.1, o bloqueio de arquivos global deve ser desativado primeiro na origem e caches associados. Para desativar, a partir do volume de origem, execute: `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- O processo para habilitar o bloqueio global de arquivos depende se a origem tem caches existentes:
  - [enable-gfl-new]
  - [enable-gfl-existing]

Habilite o bloqueio global de arquivos em novos volumes do FlexCache

Passos

1. Crie o volume FlexCache com `-is-global-file-locking` definido como verdadeiro:

   ```
   volume flexcache create volume volume_name -is-global-file-locking-enabled
   true
   ```

   > O valor padrão de `-is-global-file-locking` é "'false'". Quando quaisquer `volume flexcache create` comandos subsequentes são executados em um volume, eles devem ser passados com `-is-global-file-locking enabled` SET como "'true'".

Habilite o bloqueio global de arquivos em volumes FlexCache existentes

Passos

1. O bloqueio global de ficheiros tem de ser definido a partir do volume de origem.
2. A origem não pode ter quaisquer outras relações existentes (por exemplo, SnapMirror). Qualquer relacionamento existente deve ser dissociado. Todos os caches e volumes devem ser conetados no momento da execução do comando. Para verificar o estado da ligação, execute:

   ```
   volume flexcache connection-status show
   ```

   O status de todos os volumes listados deve ser exibido como `connected.` para obter mais informações, consulte "Exibir o status de uma relação do FlexCache" ou "Sincronizar propriedades de um volume FlexCache de uma origem".

3. Ativar o bloqueio global de ficheiros nas caches:

   ```
   volume flexcache origin config show/modify -volume volume_name -is-global-file
   -locking-enabled true
   ```

Pré-preencher um volume FlexCache

Você pode pré-preencher um volume FlexCache para reduzir o tempo necessário para acessar dados em cache.

O que você vai precisar

- Você deve ser um administrador de cluster no nível avançado de privilégio
- Os caminhos que você passa para o pré-preenchimento devem existir ou a operação de pré-preenchimento falha.

Sobre esta tarefa

- Prepovoar lê arquivos somente e rastreia através de diretórios
- O `-isRecursion` sinalizador aplica-se a toda a lista de diretórios passados para preenchimento prévio

Passos

1. Pré-preencher um volume FlexCache:

   ```
   volume flexcache prepopulate -cache-vserver vserver_name -cache-volume -path
   ```

`-list path_list -isRecursion true|false`

- O `-path-list` parâmetro indica o caminho do diretório relativo que você deseja preencher previamente a partir do diretório raiz de origem. Por exemplo, se o diretório raiz de origem for chamado /Origin e contiver diretórios /origin/dir1 e /origin/dir2, você poderá especificar a lista de caminhos da seguinte forma: `-path-list dir1, dir2` Ou `-path-list /dir1, /dir2`.
- O valor padrão `-isRecursion` do parâmetro é true.

  Este exemplo prepopula um único caminho de diretório:

  ```
  cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
  -volume fg_cachevol_1 -path-list /dir1
    (volume flexcache prepopulate start)
  [JobId 207]: FlexCache prepopulate job queued.
  ```

  Este exemplo prepopula arquivos de vários diretórios:

  ```
  cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
  -volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
    (volume flexcache prepopulate start)
  [JobId 208]: FlexCache prepopulate job queued.
  ```

  Este exemplo prepopula um único arquivo:

  ```
  cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
  -volume fg_cachevol_1 -path-list /dir1/file1.txt
    (volume flexcache prepopulate start)
  [JobId 209]: FlexCache prepopulate job queued.
  ```

  Este exemplo prepopula todos os arquivos da origem:

  ```
  cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
  -volume fg_cachevol_1 -path-list / -isRecursion true
    (volume flexcache prepopulate start)
  [JobId 210]: FlexCache prepopulate job queued.
  ```

  Este exemplo inclui um caminho inválido para o pré-preenchimento:

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
  (volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
       "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. Exibir o número de arquivos lidos:

   ```
   job show -id job_ID -ins
   ```

Eliminar uma relação FlexCache

Você pode excluir uma relação FlexCache e o volume FlexCache se não precisar mais do volume FlexCache.

Passos

1. A partir do cluster que tem o volume FlexCache, coloque o volume FlexCache offline:

   ```
   volume offline -vserver svm_name -volume volume_name
   ```

2. Eliminar o volume FlexCache:

   ```
   volume flexcache delete -vserver svm_name -volume volume_name
   ```

   Os detalhes da relação FlexCache são removidos do volume de origem e do volume FlexCache.

Gerenciamento de rede

Comece agora

Visão geral do gerenciamento de rede

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para exibir um gráfico que mostra os componentes e a configuração da sua rede, permitindo que você veja os caminhos de conexão de rede entre hosts, portas, SVMs, volumes e muito mais. A partir do ONTAP 9.12,1, você pode visualizar a associação LIF e sub-rede na grade interfaces de rede.

O gráfico é exibido quando você seleciona **rede > Visão geral** ou quando você seleciona → na seção **rede** do painel.

As seguintes categorias de componentes são mostradas no gráfico:

- Hosts
- Portas de storage
- Interfaces de rede
- VMs de storage
- Componentes de acesso a dados

Cada seção mostra detalhes adicionais sobre os quais você pode passar o Mouse ou selecionar para executar tarefas de gerenciamento e configuração de rede.

Se você estiver usando o Gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), "Gerir a rede"consulte .

Exemplos

Veja a seguir alguns exemplos das muitas maneiras de interagir com o gráfico para visualizar detalhes sobre cada componente ou iniciar ações para gerenciar sua rede:

- Clique em um host para ver sua configuração: Portas, interfaces de rede, VMs de storage e componentes de acesso a dados associados a ele.
- Passe o Mouse sobre o número de volumes em uma VM de armazenamento para selecionar um volume para exibir seus detalhes.
- Selecione uma interface iSCSI para visualizar o seu desempenho na última semana.
- Clique em ⋮ ao lado de um componente para iniciar ações para modificar esse componente.
- Determine rapidamente onde os problemas podem ocorrer em sua rede, indicado por um "X" ao lado de componentes não saudáveis.

Vídeo de visualização de rede do System Manager

Componentes de rede de uma visão geral de cluster

Você deve se familiarizar com os componentes de rede de um cluster antes de configurar o cluster. A configuração dos componentes físicos de rede de um cluster em componentes lógicos fornece a funcionalidade de flexibilidade e alocação a vários clientes no ONTAP.

Os vários componentes de rede em um cluster são os seguintes:

- Portas físicas

  Placas de interface de rede (NICs) e adaptadores de barramento de host (HBAs) fornecem conexões físicas (Ethernet e Fibre Channel) de cada nó para as redes físicas (redes de gerenciamento e dados).

  Para obter informações sobre os requisitos do local, informações sobre o switch, informações sobre o cabeamento da porta integrada da controladora e o cabeamento da porta integrada, consulte o Hardware Universe em "hwu.NetApp.com".

- Portas lógicas

  As redes de área local virtual (VLANs) e os grupos de interface constituem as portas lógicas. Os grupos de interface tratam várias portas físicas como uma única porta, enquanto as VLANs subdividem uma porta física em várias portas separadas.

- IPspaces

  Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

- Domínios de broadcast

  Um domínio de broadcast reside em um IPspace e contém um grupo de portas de rede, potencialmente de muitos nós no cluster, que pertencem à mesma rede de camada 2. As portas do grupo são usadas em uma SVM para tráfego de dados.

- Sub-redes

  Uma sub-rede é criada dentro de um domínio de broadcast e contém um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Esse conjunto de endereços IP simplifica a alocação de endereços IP durante a criação de LIF.

- Interfaces lógicas

  Uma interface lógica (LIF) é um endereço IP ou um nome de porta mundial (WWPN) associado a uma porta. Ela está associada a atributos como grupos de failover, regras de failover e regras de firewall. Um LIF se comunica através da rede através da porta (física ou lógica) à qual está atualmente vinculado.

  Os diferentes tipos de LIFs em um cluster são LIFs de dados, LIFs de gerenciamento com escopo de cluster, LIFs de gerenciamento com escopo de nó, LIFs entre clusters e LIFs de cluster. A propriedade dos LIFs depende do SVM onde o LIF reside. Os data LIFs são propriedade de Data SVMs, LIFs de gerenciamento com escopo de nó, gerenciamento com escopo de cluster e LIFs entre clusters são de propriedade das SVMs de administrador e os LIFs de cluster são de propriedade do cluster SVM.

- Zonas DNS

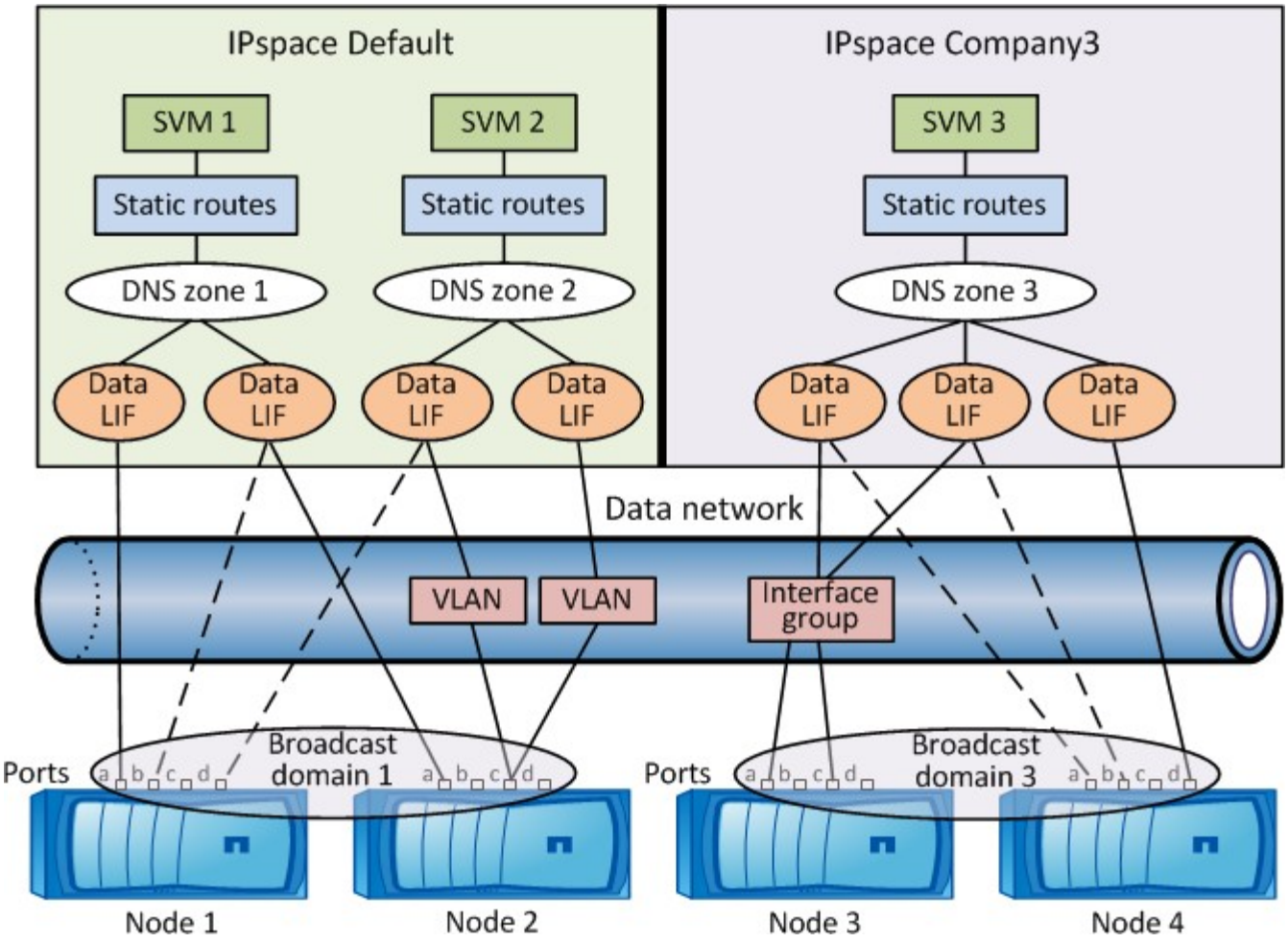
  A zona DNS pode ser especificada durante a criação do LIF, fornecendo um nome para o LIF ser exportado através do servidor DNS do cluster. Vários LIFs podem compartilhar o mesmo nome, permitindo que o recurso de balanceamento de carga DNS distribua endereços IP para o nome de acordo com a carga.

  Os SVMs podem ter várias zonas DNS.

- Roteamento

  Cada SVM é autossuficiente em relação à rede. Um SVM possui LIFs e rotas que podem alcançar cada um dos servidores externos configurados.

  A figura a seguir ilustra como os diferentes componentes de rede estão associados em um cluster de quatro nós:

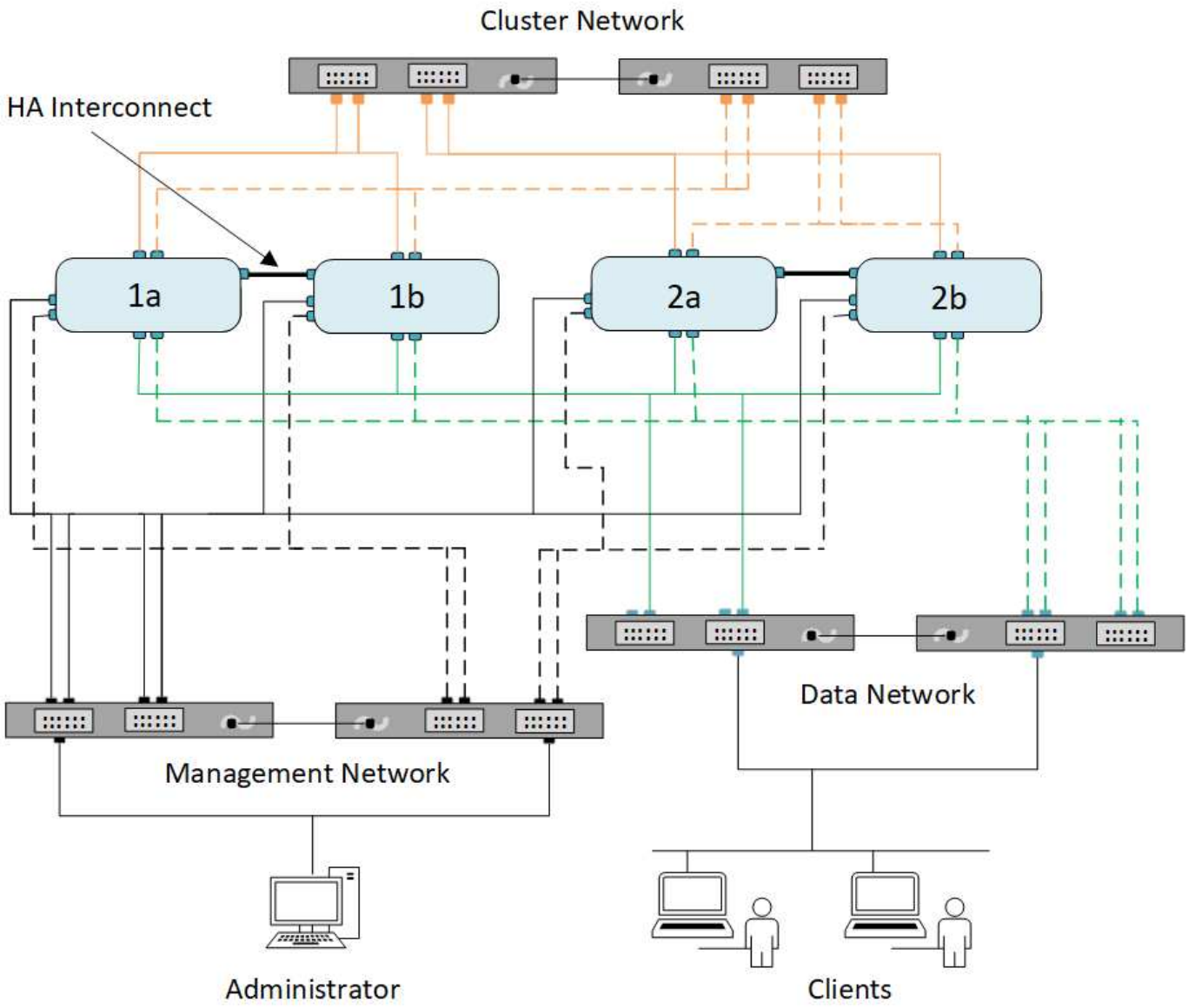


Diretrizes de cabeamento de rede

As práticas recomendadas de cabeamento de rede separam o tráfego nas seguintes redes: Cluster, gerenciamento e dados.

Você deve fazer um cabeamento de um cluster para que o tráfego do cluster esteja em uma rede separada de todo o outro tráfego. É uma prática opcional, mas recomendada, separar o tráfego de gerenciamento de rede dos dados e do tráfego entre clusters. Ao manter redes separadas, você pode obter melhor desempenho, facilidade de administração e maior segurança e acesso de gerenciamento aos nós.

O diagrama a seguir ilustra o cabeamento de rede de um cluster HA de quatro nós que inclui três redes separadas:



Você deve seguir certas diretrizes ao fazer cabeamento de conexões de rede:

- Cada nó deve ser conetado a três redes distintas.

  Uma rede é para gerenciamento, outra para acesso aos dados e outra para comunicação entre clusters. A gestão e as redes de dados podem ser logicamente separadas.

- Você pode ter mais de uma conexão de rede de dados para cada nó para melhorar o fluxo de tráfego do cliente (dados).
- Um cluster pode ser criado sem conexões de rede de dados, mas deve incluir uma conexão de interconexão de cluster.
- Sempre deve haver duas ou mais conexões de cluster para cada nó.

Para obter mais informações sobre cabeamento de rede, consulte "Centro de Documentação do sistema AFF e FAS" e "Hardware Universe" .

Relação entre domínios de broadcast, grupos de failover e políticas de failover

Domínios de broadcast, grupos de failover e políticas de failover trabalham em conjunto para determinar qual porta assumirá quando o nó ou a porta na qual um LIF é configurado falhar.

Um domínio de broadcast lista todas as portas alcançáveis na mesma rede Ethernet de camada 2. Um pacote de broadcast Ethernet enviado de uma das portas é visto por todas as outras portas no domínio de broadcast. Essa caraterística de acessibilidade comum de um domínio de broadcast é importante para LIFs porque se um LIF falhasse para qualquer outra porta no domínio de broadcast, ele ainda poderia alcançar todos os hosts locais e remotos que estavam acessíveis a partir da porta original.

Os grupos de failover definem as portas dentro de um domínio de broadcast que fornecem cobertura de failover de LIF entre si. Cada domínio de broadcast tem um grupo de failover que inclui todas as suas portas. Esse grupo de failover que contém todas as portas no domínio de broadcast é o grupo de failover padrão e recomendado para o LIF. Você pode criar grupos de failover com subconjuntos menores que você definir, como um grupo de portas de failover que têm a mesma velocidade de link em um domínio de broadcast.

Uma política de failover dita como um LIF usa as portas de um grupo de failover quando um nó ou porta é desativado. Considere a política de failover como um tipo de filtro aplicado a um grupo de failover. Os destinos de failover para um LIF (o conjunto de portas para as quais um LIF pode fazer failover) são determinados aplicando a política de failover de LIF ao grupo de failover de LIF no domínio de broadcast.

Você pode exibir os destinos de failover para um LIF usando o seguinte comando CLI:

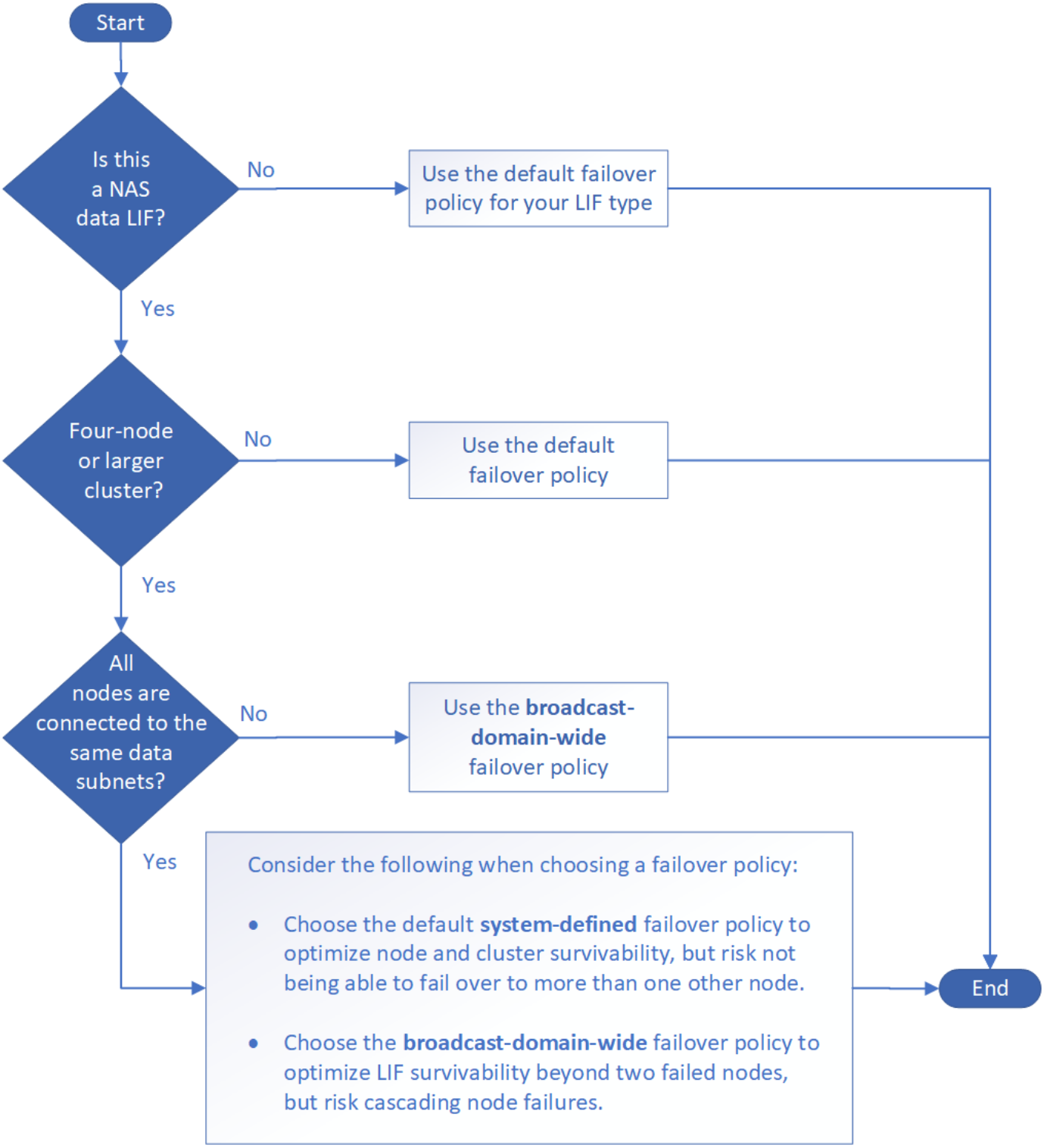
```
network interface show -failover
```

O NetApp recomenda fortemente o uso da política de failover padrão para o seu tipo de LIF.

Decida qual política de failover de LIF usar

Decida se deseja usar a política de failover padrão recomendada ou se deseja alterá-la com base no seu tipo e ambiente de LIF.

Árvore de decisões de política de failover



Políticas de failover padrão por tipo de LIF

Tipo de LIF	Política de failover padrão	Descrição
BGP LIFs	desativado	O LIF não faz failover para outra porta.
LIFs de cluster	apenas local	O LIF faz failover para portas apenas no mesmo nó.
LIF de cluster-mgmt	broadcast-domain-wide	O LIF faz failover para portas no mesmo domínio de broadcast, em todos e em todos os nós do cluster.

LIFs entre clusters	apenas local	O LIF faz failover para portas apenas no mesmo nó.
LIFs de dados nas	definido pelo sistema	O LIF faz failover para um outro nó que não é o parceiro de HA.
LIFs de gerenciamento de nós	apenas local	O LIF faz failover para portas apenas no mesmo nó.
LIFs de dados SAN	desativado	O LIF não faz failover para outra porta.

A política de failover "somente para parceiros sfo" não é padrão, mas pode ser usada quando você deseja que o LIF faça failover para uma porta no nó inicial ou apenas para parceiros SFO.

Fluxo de trabalho de failover de caminho nas (ONTAP 9.8 e posterior)

Sobre o failover de caminho nas (ONTAP 9.8 e posterior)

Esse fluxo de trabalho orienta você pelas etapas de configuração de rede para configurar o failover de caminho nas para o ONTAP 9.8 e posterior. Este fluxo de trabalho assume o seguinte:

- Você deseja usar as práticas recomendadas de failover de caminho nas em um fluxo de trabalho que simplifica a configuração de rede.
- Você deseja usar a CLI, não o System Manager.
- Você está configurando a rede em um novo sistema executando o ONTAP 9.8 ou posterior.

Se você estiver executando uma versão do ONTAP anterior a 9,8, use o seguinte procedimento de failover de caminho do nas para ONTAP 9.0 a 9,7:

- "Fluxo de trabalho de failover de caminho nas ONTAP 9.0-9,7"

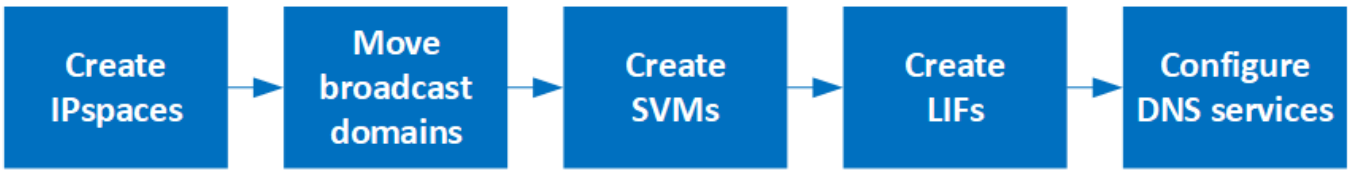
Se você quiser detalhes de gerenciamento de rede, use o material de referência de gerenciamento de rede:

- Visão geral do gerenciamento de rede

Fluxo de trabalho (ONTAP 9.8 e posterior)

Se você já estiver familiarizado com os conceitos básicos de rede, poderá economizar tempo configurando sua rede revisando esse fluxo de trabalho "prático" para a configuração de failover de caminho nas.

Um LIF nas migra automaticamente para uma porta de rede sobrevivente após uma falha de link em sua porta atual. Você pode confiar nos padrões do ONTAP para gerenciar o failover de caminho.



Um SAN LIF não migra (a menos que você o mova manualmente após a falha do link). Em vez disso, a tecnologia multipathing no host desvia o tráfego para um LIF diferente. Para obter mais informações, "Administração da SAN"consulte .

1. **"Complete a Planilha"**

Use a Planilha para Planejar o failover de caminho nas.

2. **"Crie IPspaces"**

Crie um espaço de endereço IP distinto para cada SVM em um cluster.

3. **"Mover domínios de broadcast para IPspaces"**

Mover domínios de broadcast para IPspaces.

4. **"Crie SVMs"**

Crie SVMs para fornecer dados aos clientes.

5. **"Crie LIFs"**

Crie LIFs nas portas que você deseja usar para acessar dados.

6. **"Configurar serviços DNS para o SVM"**

Configure os serviços DNS para o SVM antes de criar um servidor NFS ou SMB.

Planilha para configuração de failover de caminho nas (ONTAP 9.8 e posterior)

Você deve concluir todas as seções da Planilha antes de configurar o failover de caminho nas.

Configuração IPspace

Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Informações	Obrigatório?	Seus valores
IPspace name o identificador exclusivo do IPspace.	Sim	

Configuração do domínio de difusão

Um domínio de broadcast agrupa portas que pertencem à mesma rede de camada 2 e define a MTU para as

portas do domínio de broadcast.

Os domínios de broadcast são atribuídos a um IPspace. Um IPspace pode conter um ou mais domínios de broadcast.

> A porta para a qual um LIF falha deve ser membro do grupo de failover para o LIF. Para cada domínio de broadcast criado pelo ONTAP, também é criado um grupo de failover com o mesmo nome que contém todas as portas no domínio de broadcast.

Informações	Obrigatório?	Seus valores
IPspace name o IPspace ao qual o domínio de broadcast é atribuído. Este espaço IPspace tem de existir.	Sim	
Nome de domínio de broadcast o nome do domínio de broadcast. Esse nome deve ser único no IPspace.	Sim	
MTU o valor máximo da unidade de transmissão para o domínio de transmissão, normalmente definido como **1500** ou **9000**. O valor MTU é aplicado a todas as portas no domínio de broadcast e a todas as portas que forem adicionadas posteriormente ao domínio de broadcast. O valor MTU deve corresponder a todos os dispositivos ligados a essa rede. Observe que o gerenciamento de gerenciamento de portas e0M e o tráfego do processador de serviços devem ter o MTU definido para não mais de 1500 bytes.	Sim	
As portas são atribuídas a domínios de broadcast com base na acessibilidade. Depois que a atribuição de porta estiver concluída, verifique a acessibilidade executando o `network port reachability show` comando. Essas portas podem ser portas físicas, VLANs ou grupos de interface.	Sim	

Configuração de sub-rede

Uma sub-rede contém pools de endereços IP e um gateway padrão que pode ser atribuído a LIFs usados por SVMs residentes no IPspace.

- Ao criar um LIF em uma SVM, você pode especificar o nome da sub-rede em vez de fornecer um endereço IP e uma sub-rede.
- Como uma sub-rede pode ser configurada com um gateway padrão, você não precisa criar o gateway padrão em uma etapa separada ao criar um SVM.
- Um domínio de broadcast pode conter uma ou mais sub-redes.
- Você pode configurar LIFs SVM que estão em sub-redes diferentes associando mais de uma sub-rede ao domínio de broadcast do IPspace.
- Cada sub-rede deve conter endereços IP que não se sobreponham aos endereços IP atribuídos a outras sub-redes no mesmo espaço IPspace.
- Você pode atribuir endereços IP específicos a LIFs de dados do SVM e criar um gateway padrão para o SVM em vez de usar uma sub-rede.

Informações	Obrigatório?	Seus valores
IPspace name o IPspace ao qual a sub-rede será atribuída. Este espaço IPspace tem de existir.	Sim	
Nome da sub-rede o nome da sub-rede. Esse nome deve ser único no IPspace.	Sim	
Nome de domínio de broadcast o domínio de broadcast ao qual a sub-rede será atribuída. Esse domínio de broadcast deve residir no espaço IPspace especificado.	Sim	
Nome da sub-rede e mascarar a sub-rede e a máscara em que residem os endereços IP.	Sim	
Gateway você pode especificar um gateway padrão para a sub-rede. Se você não atribuir um gateway ao criar a sub-rede, poderá atribuir um mais tarde.	Não	

Intervalos de endereços IP você pode especificar um intervalo de endereços IP ou endereços IP específicos. Por exemplo, você pode especificar um intervalo como: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` Se você não especificar um intervalo de endereços IP, todo o intervalo de endereços IP na sub-rede especificada estará disponível para atribuir a LIFs.	Não	
Force update of LIF associations especifica se deve forçar a atualização das associações de LIF existentes. Por padrão, a criação de sub-rede falhará se qualquer interface de processador de serviço ou interfaces de rede estiver usando os endereços IP nos intervalos fornecidos. O uso deste parâmetro associa quaisquer interfaces endereçadas manualmente à sub-rede e permite que o comando seja bem-sucedido.	Não	

Configuração SVM

Você usa SVMs para fornecer dados a clientes e hosts.

Os valores que você Registra são para criar um SVM de dados padrão. Se você estiver criando uma SVM de origem MetroCluster, consulte "Guia de instalação e configuração do MetroCluster conectado à malha"ou "Guia de instalação e configuração do Stretch MetroCluster".

Informações	Obrigatório?	Seus valores
SVM nomeie o nome de domínio totalmente qualificado (FQDN) do SVM. Esse nome deve ser único em ligas de cluster.	Sim	
Nome do volume raiz o nome do volume raiz do SVM.	Sim	
Agregar nome o nome do agregado que contém o volume raiz da SVM. Este agregado deve existir.	Sim	
Estilo de segurança o estilo de segurança do volume raiz da SVM. Os valores possíveis são **NTFS**, **unix** e **Mixed**.	Sim	

IPspace nomeie o IPspace ao qual o SVM é atribuído. Este espaço IPspace tem de existir.	Não	
Linguagem SVM que define o idioma padrão a ser usado para o SVM e seus volumes. Se você não especificar um idioma padrão, o idioma SVM padrão será definido como **C.UTF-8**. A configuração de idioma SVM determina o conjunto de carateres usado para exibir nomes e dados de arquivos para todos os volumes nas no SVM. Você pode modificar o idioma após a criação do SVM.	Não	

Configuração LIF

Um SVM fornece dados a clientes e hosts por meio de uma ou mais interfaces lógicas de rede (LIFs).

Informações	Obrigatório?	Seus valores
SVM nomeie o nome do SVM para o LIF.	Sim	
LIF nome o nome do LIF. Você pode atribuir várias LIFs de dados por nó e pode atribuir LIFs a qualquer nó no cluster, desde que o nó tenha portas de dados disponíveis. Para fornecer redundância, você deve criar pelo menos duas LIFs de dados para cada sub-rede de dados e as LIFs atribuídas a uma sub-rede específica devem ser atribuídas portas residenciais em diferentes nós. **Importante:** se você estiver configurando um servidor SMB para hospedar Hyper-V ou SQL Server em SMB para soluções de operação sem interrupções, o SVM deve ter pelo menos um LIF de dados em cada nó no cluster.	Sim	
Política de serviço Política de serviço para o LIF. A política de serviço define quais serviços de rede podem usar o LIF. Serviços incorporados e políticas de serviço estão disponíveis para gerenciar dados e tráfego de gerenciamento em SVMs de dados e do sistema.	Sim	
Os LIFs baseados em IP não exigem protocolos permitidos, use a linha de diretiva de serviço. Especifique protocolos permitidos para SAN LIFs em portas Fibre Channel. Estes são os protocolos que podem usar esse LIF. Os protocolos que usam o LIF não podem ser modificados após a criação do LIF. Você deve especificar todos os protocolos ao configurar o LIF.	Não	

Nó inicial o nó para o qual o LIF retorna quando o LIF é revertido para sua porta inicial. Você deve gravar um nó inicial para cada LIF de dados.	Sim	
A porta inicial ou domínio de broadcast escolheu um dos seguintes: **Port**: Especifique a porta para a qual a interface lógica retorna quando o LIF é revertido para sua porta inicial. Isso só é feito para o primeiro LIF na sub-rede de um espaço IPspace, caso contrário, não é necessário. **Domínio de transmissão**: Especifique o domínio de transmissão e o sistema selecionará a porta apropriada para a qual a interface lógica retorna quando o LIF é revertido para sua porta inicial.	Sim	
Subrede nomeie a sub-rede a ser atribuída ao SVM. Todas as LIFs de dados usadas para criar conexões SMB continuamente disponíveis para servidores de aplicativos devem estar na mesma sub-rede.	Sim (se estiver usando uma sub-rede)	

Configuração DNS

Você deve configurar o DNS na SVM antes de criar um servidor NFS ou SMB.

Informações	Obrigatório?	Seus valores
SVM nomeie o nome do SVM no qual você deseja criar um servidor NFS ou SMB.	Sim	
Nome de domínio DNS Uma lista de nomes de domínio a anexar a um nome de host ao executar a resolução de nome de host para IP. Liste primeiro o domínio local, seguido pelos nomes de domínio para os quais as consultas DNS são mais frequentemente feitas.	Sim	

Endereços IP dos servidores DNS Lista de endereços IP para os servidores DNS que fornecem resolução de nomes para o servidor NFS ou SMB. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor SMB irá ingressar. O Registro SRV é usado para mapear o nome de um serviço para o nome de computador DNS de um servidor que oferece esse serviço. A criação do servidor SMB falhará se o ONTAP não conseguir obter os Registros de localização do serviço por meio de consultas DNS locais. A maneira mais simples de garantir que o ONTAP possa localizar os Registros SRV do ative Directory é configurar servidores DNS integrados ao ative Directory como servidores DNS SVM. Você pode usar servidores DNS não integrados ao ative Directory desde que o administrador DNS tenha adicionado manualmente os Registros SRV à zona DNS que contém informações sobre os controladores de domínio do ative Directory. Para obter informações sobre os Registros SRV integrados ao ative Directory, consulte o "Como o suporte DNS para ative Directory funciona no Microsoft TechNet"tópico .	Sim	

Configuração de DNS dinâmico

Antes de poder utilizar o DNS dinâmico para adicionar automaticamente entradas de DNS aos servidores DNS integrados do ative Directory, tem de configurar o DNS dinâmico (DDNS) no SVM.

Registros DNS são criados para cada LIF de dados na SVM. Ao criar vários dados LIFS no SVM, você pode equilibrar as conexões de clientes com os endereços IP de dados atribuídos. A carga de DNS equilibra as conexões que são feitas usando o nome do host para os endereços IP atribuídos de forma redonda.

Informações	Obrigatório?	Seus valores
SVM nomeie o SVM no qual você deseja criar um servidor NFS ou SMB.	Sim	
Se usar o DDNS especifica se deve-se usar o DDNS. Os servidores DNS configurados no SVM devem oferecer suporte a DDNS. Por padrão, o DDNS está desativado.	Sim	

Se usar DDNS seguro o DDNS seguro é suportado apenas com DNS integrado ao ative Directory. Se o DNS integrado ao ative Directory permitir apenas atualizações seguras de DDNS, o valor deste parâmetro deve ser verdadeiro. Por padrão, o DDNS seguro está desativado. O DDNS seguro só pode ser ativado depois de um servidor SMB ou uma conta do ative Directory ter sido criada para o SVM.	Não	
FQDN do domínio DNS o FQDN do domínio DNS. Você deve usar o mesmo nome de domínio configurado para serviços de nome DNS na SVM.	Não	

Fluxo de trabalho de failover de caminho nas (ONTAP 9.7 e anterior)

Configurar failover de caminho nas (ONTAP 9 .7 e anterior)

Esse fluxo de trabalho orienta você pelas etapas de configuração de rede para configurar o failover de caminho nas para o ONTAP 9.0 - 9,7. Este fluxo de trabalho assume o seguinte:

- Você deseja usar as práticas recomendadas de failover de caminho nas que simplificam a configuração de rede.
- Você deseja usar a CLI, não o System Manager.
- Você está configurando a rede em um novo sistema executando o ONTAP 9.0 a 9,7.

Se você estiver executando uma versão do ONTAP posterior a 9,7, use o procedimento de failover de caminho nas para o ONTAP 9.8 ou posterior:

- Fluxo de trabalho de failover de caminho nas do ONTAP 9.8 e posterior

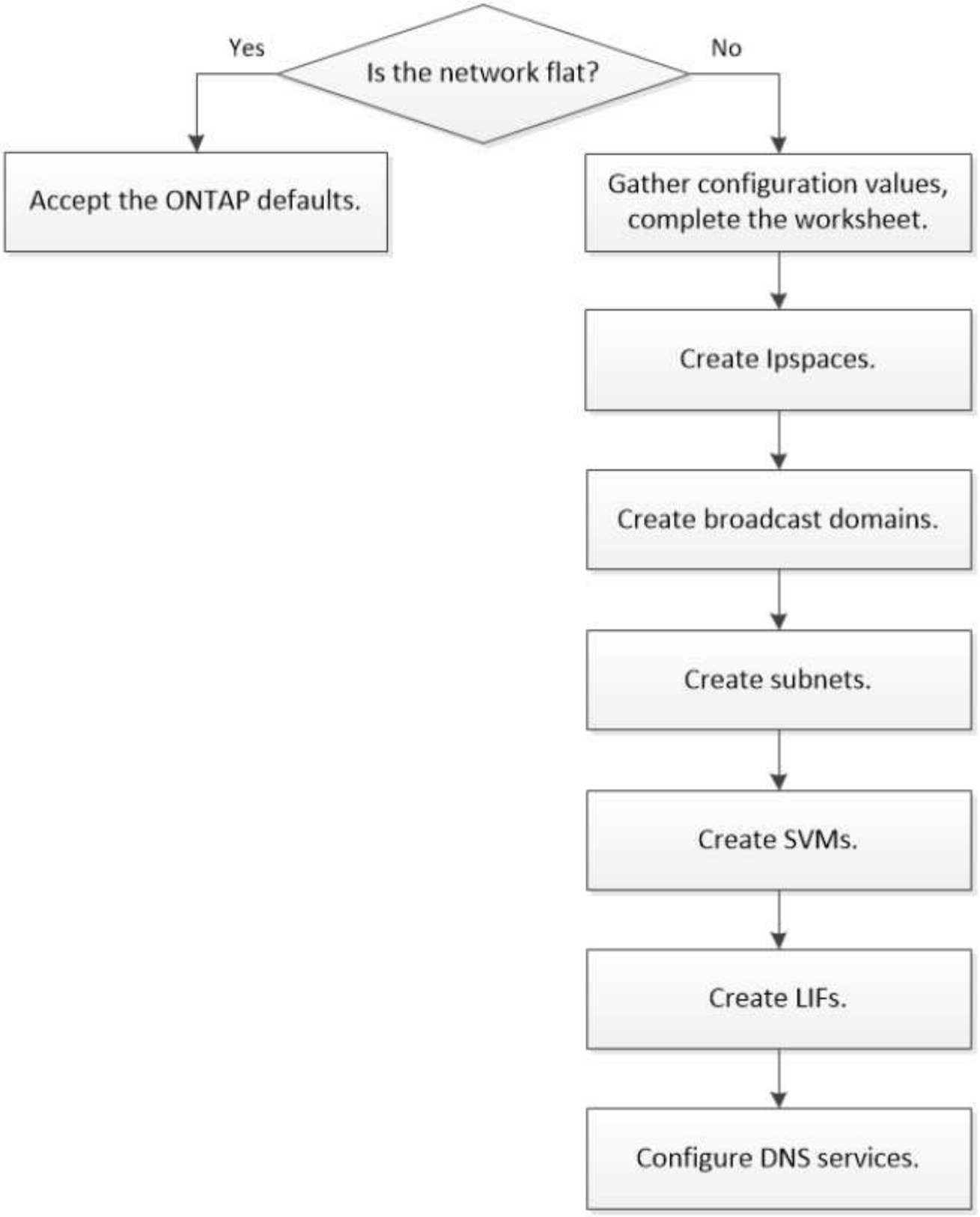
Se você quiser detalhes sobre componentes e gerenciamento de rede, use o material de referência de gerenciamento de rede:

- Visão geral do gerenciamento de rede

Fluxo de trabalho (ONTAP 9 .7 e anterior)

Se você já estiver familiarizado com os conceitos básicos de rede, poderá economizar tempo configurando sua rede revisando esse fluxo de trabalho "prático" para a configuração de failover de caminho nas.

Um LIF nas migra automaticamente para uma porta de rede sobrevivente após uma falha de link em sua porta atual. Se sua rede estiver plana, você poderá confiar nos padrões do ONTAP para gerenciar o failover de caminho. Caso contrário, você deve configurar o failover de caminho seguindo as etapas deste fluxo de trabalho.



Um SAN LIF não migra (a menos que você o mova manualmente após a falha do link). Em vez disso, a tecnologia multipathing no host desvia o tráfego para um LIF diferente. Para obter mais informações, "Administração da SAN"consulte .

1 **"Complete a Planilha"**

Use a Planilha para Planejar o failover de caminho nas.

2 **"Crie IPspaces"**

Crie um espaço de endereço IP distinto para cada SVM em um cluster.

3 **"Criar domínios de broadcast"**

Criar domínios de broadcast.

4 **"Crie sub-redes"**

Crie sub-redes.

5 **"Crie SVMs"**

Crie SVMs para fornecer dados aos clientes.

6 **"Crie LIFs"**

Crie LIFs nas portas que você deseja usar para acessar dados.

7 **"Configurar serviços DNS para o SVM"**

Configure os serviços DNS para o SVM antes de criar um servidor NFS ou SMB.

Planilha para a configuração de failover de caminho nas (ONTAP 9.7 e anterior)

Você deve concluir todas as seções da Planilha antes de configurar o failover de caminho nas.

Configuração IPspace

Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Informações	Obrigatório?	Seus valores
Nome do IPspace • O nome do IPspace. • O nome deve ser exclusivo no cluster.	Sim	

Configuração do domínio de difusão

Um domínio de broadcast agrupa portas que pertencem à mesma rede de camada 2 e define a MTU para as portas do domínio de broadcast.

Os domínios de broadcast são atribuídos a um IPspace. Um IPspace pode conter um ou mais domínios de broadcast.

> A porta para a qual um LIF falha deve ser membro do grupo de failover para o LIF. Quando você cria um domínio de broadcast, o ONTAP cria automaticamente um grupo de failover com o mesmo nome. O grupo failover contém todas as portas atribuídas ao domínio de broadcast.

Informações	Obrigatório?	Seus valores
Nome do IPspace • O espaço IPspace ao qual o domínio de broadcast é atribuído. • O espaço IPspace deve existir.	Sim	
Nome de domínio de broadcast • O nome do domínio de difusão. • Esse nome deve ser único no IPspace.	Sim	

MTU • A MTU do domínio de broadcast. • Normalmente definido para **1500** ou **9000**. • O valor MTU é aplicado a todas as portas no domínio de broadcast e a todas as portas que forem adicionadas posteriormente ao domínio de broadcast. O valor MTU deve corresponder a todos os dispositivos ligados a essa rede. Observe que o gerenciamento de gerenciamento de portas e0M e o tráfego do processador de serviços devem ter o MTU definido para não mais de 1500 bytes.	Sim	
Portas • As portas de rede a serem adicionadas ao domínio de broadcast. • As portas atribuídas ao domínio de broadcast podem ser portas físicas, VLANs ou grupos de interface (ifgroups). • Se uma porta estiver em outro domínio de broadcast, ela deve ser removida antes que ela possa ser adicionada ao domínio de broadcast. • As portas são atribuídas especificando o nome do nó e a porta: Por exemplo, node1:e0d.	Sim	

Configuração de sub-rede

Uma sub-rede contém pools de endereços IP e um gateway padrão que pode ser atribuído a LIFs usados por SVMs residentes no IPspace.

- Ao criar um LIF em uma SVM, você pode especificar o nome da sub-rede em vez de fornecer um endereço IP e uma sub-rede.
- Como uma sub-rede pode ser configurada com um gateway padrão, você não precisa criar o gateway padrão em uma etapa separada ao criar um SVM.
- Um domínio de broadcast pode conter uma ou mais sub-redes. Você pode configurar LIFs SVM que estão em sub-redes diferentes associando mais de uma sub-rede ao domínio de broadcast do IPspace.
- Cada sub-rede deve conter endereços IP que não se sobreponham aos endereços IP atribuídos a outras sub-redes no mesmo espaço IPspace.
- Você pode atribuir endereços IP específicos a LIFs de dados do SVM e criar um gateway padrão para o SVM em vez de usar uma sub-rede.

Informações	Obrigatório?	Seus valores
Nome do IPspace • O espaço IPspace ao qual a sub-rede será atribuída. • O espaço IPspace deve existir.	Sim	
Nome da sub-rede • O nome da sub-rede. • O nome deve ser único no IPspace.	Sim	
Nome de domínio de broadcast • O domínio de broadcast ao qual a sub-rede será atribuída. • O domínio de broadcast deve residir no espaço IPspace especificado.	Sim	
Nome e máscara da sub-rede • A sub-rede e a máscara em que os endereços IP residem.	Sim	

Gateway • Você pode especificar um gateway padrão para a sub-rede. • Se você não atribuir um gateway ao criar a sub-rede, poderá atribuir um à sub-rede a qualquer momento.	Não	
Intervalos de endereços IP • Você pode especificar um intervalo de endereços IP ou endereços IP específicos. Por exemplo, você pode especificar um intervalo como: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` • Se você não especificar um intervalo de endereços IP, todo o intervalo de endereços IP na sub-rede especificada estará disponível para atribuir a LIFs.	Não	
Forçar atualização de associações de LIF • Especifica se deve-se forçar a atualização das associações de LIF existentes. • Por padrão, a criação de sub-rede falhará se qualquer interface de processador de serviço ou interfaces de rede estiver usando os endereços IP nos intervalos fornecidos. • O uso deste parâmetro associa quaisquer interfaces endereçadas manualmente à sub-rede e permite que o comando seja bem-sucedido.	Não	

Configuração SVM

Você usa SVMs para fornecer dados a clientes e hosts.

Os valores que você Registra são para criar um SVM de dados padrão. Se você estiver criando uma SVM de

origem MetroCluster, consulte "Instale um MetroCluster conectado à malha"ou "Instale um Stretch MetroCluster".

Informações	Obrigatório?	Seus valores
Nome do SVM • O nome do SVM. • Você deve usar um nome de domínio totalmente qualificado (FQDN) para garantir nomes exclusivos de SVM em ligas de cluster.	Sim	
Nome do volume raiz • O nome do volume raiz do SVM.	Sim	
Nome agregado • O nome do agregado que contém o volume raiz da SVM. • Este agregado deve existir.	Sim	
Estilo de segurança • O estilo de segurança do volume raiz da SVM. • Os valores possíveis são **NTFS**, **unix** e **Mixed**.	Sim	
Nome do IPspace • O IPspace ao qual o SVM é atribuído. • Este espaço IPspace tem de existir.	Não	

Configuração de idioma SVM • O idioma padrão a ser usado para o SVM e seus volumes. • Se você não especificar um idioma padrão, o idioma SVM padrão será definido como **C.UTF-8**. • A configuração de idioma SVM determina o conjunto de carateres usado para exibir nomes e dados de arquivos para todos os volumes nas no SVM. Você pode modificar o idioma após a criação do SVM.	Não	

Configuração LIF

Um SVM fornece dados a clientes e hosts por meio de uma ou mais interfaces lógicas de rede (LIFs).

Informações	Obrigatório?	Seus valores
Nome do SVM • O nome do SVM para o LIF.	Sim	
Nome LIF • O nome do LIF. • Você pode atribuir várias LIFs de dados por nó e pode atribuir LIFs a qualquer nó no cluster, desde que o nó tenha portas de dados disponíveis. • Para fornecer redundância, você deve criar pelo menos duas LIFs de dados para cada sub-rede de dados e as LIFs atribuídas a uma sub-rede específica devem ser atribuídas portas residenciais em diferentes nós. **Importante:** se você estiver configurando um servidor SMB para hospedar Hyper-V ou SQL Server em SMB para soluções de operação sem interrupções, o SVM deve ter pelo menos um LIF de dados em cada nó no cluster.	Sim	

Função do LIF • O papel do LIF. • Os LIFs de dados recebem a função de dados.	Sim Decoreated from ONTAP 9.6	dados
Política de serviço Política de serviço para o LIF. A política de serviço define quais serviços de rede podem usar o LIF. Serviços incorporados e políticas de serviço estão disponíveis para gerenciar dados e tráfego de gerenciamento em SVMs de dados e do sistema.	Sim começando com ONTAP 9.6	
Protocolos permitidos • Os protocolos que podem usar o LIF. • Por padrão, SMB, NFS e FlexCache são permitidos. O protocolo FlexCache permite que um volume seja usado como um volume de origem para um volume FlexCache em um sistema executando o Data ONTAP operando no modo 7D. Os protocolos que usam o LIF não podem ser modificados após a criação do LIF. Você deve especificar todos os protocolos ao configurar o LIF.	Não	
Nó inicial • O nó para o qual o LIF retorna quando o LIF é revertido para sua porta inicial. • Você deve gravar um nó inicial para cada LIF de dados.	Sim	

Porta inicial ou domínio de broadcast • A porta para a qual a interface lógica retorna quando o LIF é revertido para sua porta inicial. • Você deve gravar uma porta inicial para cada LIF de dados.	Sim	
Nome da sub-rede • A sub-rede a atribuir ao SVM. • Todas as LIFs de dados usadas para criar conexões SMB continuamente disponíveis para servidores de aplicativos devem estar na mesma sub-rede.	Sim (se estiver usando uma sub-rede)	

Configuração DNS

Você deve configurar o DNS na SVM antes de criar um servidor NFS ou SMB.

Informações	Obrigatório?	Seus valores
Nome do SVM • O nome do SVM no qual você deseja criar um servidor NFS ou SMB.	Sim	
Nome de domínio DNS • Uma lista de nomes de domínio a anexar a um nome de host ao executar a resolução de nome de host para IP. • Liste primeiro o domínio local, seguido pelos nomes de domínio para os quais as consultas DNS são mais frequentemente feitas.	Sim	

Endereços IP dos servidores DNS • Lista de endereços IP para os servidores DNS que fornecerão a resolução de nomes para o servidor NFS ou SMB. • Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor SMB irá ingressar. O Registro SRV é usado para mapear o nome de um serviço para o nome de computador DNS de um servidor que oferece esse serviço. A criação do servidor SMB falhará se o ONTAP não conseguir obter os Registros de localização do serviço por meio de consultas DNS locais. A maneira mais simples de garantir que o ONTAP possa localizar os Registros SRV do ative Directory é configurar servidores DNS integrados ao ative Directory como servidores DNS SVM. Você pode usar servidores DNS não integrados ao ative Directory desde que o administrador DNS tenha adicionado manualmente os Registros SRV à zona DNS que contém informações sobre os controladores de domínio do ative Directory. • Para obter informações sobre os Registros SRV integrados ao ative Directory, consulte o "Como o suporte DNS para ative Directory funciona no Microsoft TechNet"tópico .	Sim	

Configuração de DNS dinâmico

Antes de poder utilizar o DNS dinâmico para adicionar automaticamente entradas de DNS aos servidores DNS integrados do ative Directory, tem de configurar o DNS dinâmico (DDNS) no SVM.

Registros DNS são criados para cada LIF de dados na SVM. Ao criar vários dados LIFS no SVM, você pode

equilibrar as conexões de clientes com os endereços IP de dados atribuídos. A carga de DNS equilibra as conexões que são feitas usando o nome do host para os endereços IP atribuídos de forma redonda.

Informações	Obrigatório?	Seus valores
Nome do SVM • SVM no qual você deseja criar um servidor NFS ou SMB.	Sim	
Se deve usar DDNS • Especifica se o DDNS deve ser usado. • Os servidores DNS configurados no SVM devem oferecer suporte a DDNS. Por padrão, o DDNS está desativado.	Sim	
Se usar DDNS seguro • O DDNS seguro é suportado apenas com DNS integrado ao ative Directory. • Se o DNS integrado ao ative Directory permitir apenas atualizações seguras de DDNS, o valor deste parâmetro deve ser verdadeiro. • Por padrão, o DDNS seguro está desativado. • O DDNS seguro só pode ser ativado depois de um servidor SMB ou uma conta do ative Directory ter sido criada para o SVM.	Não	
FQDN do domínio DNS • O FQDN do domínio DNS. • Você deve usar o mesmo nome de domínio configurado para serviços de nome DNS na SVM.	Não	

Portas de rede

Configurar a visão geral das portas de rede

As portas são portas físicas (NICs) ou portas virtualizadas, como grupos de interfaces ou VLANs.

As redes de área local virtual (VLANs) e os grupos de interface constituem as portas virtuais. Os grupos de interface tratam várias portas físicas como uma única porta, enquanto as VLANs subdividem uma porta física em várias portas lógicas separadas.

- Portas físicas: LIFs podem ser configuradas diretamente em portas físicas.
- Grupo de interfaces: Um agregado de portas contendo duas ou mais portas físicas que atuam como uma única porta de tronco. Um grupo de interfaces pode ser multimodo, monomodo ou dinâmico.
- VLAN: Uma porta lógica que recebe e envia tráfego com tag VLAN (padrão IEEE 802,1Q.1ad). As caraterísticas da porta VLAN incluem o ID da VLAN para a porta. A porta física subjacente ou as portas do grupo de interfaces são consideradas portas de tronco VLAN, e as portas do switch conetado devem ser configuradas para ramificar os IDs de VLAN.

  A porta física subjacente ou as portas do grupo de interfaces para uma porta VLAN podem continuar hospedando LIFs, que transmitem e recebem tráfego não marcado.

- Porta IP virtual (VIP): Uma porta lógica que é usada como porta inicial para um LIF VIP. As portas VIP são criadas automaticamente pelo sistema e suportam apenas um número limitado de operações. As portas VIP são suportadas a partir do ONTAP 9.5.

A convenção de nomenclatura de portas é *enumberletter*:

- O primeiro caractere descreve o tipo de porta. "E" representa Ethernet.
- O segundo caractere indica o slot numerado no qual o adaptador de porta está localizado.
- O terceiro caractere indica a posição da porta em um adaptador multiporta. "a" indica a primeira porta, "b" indica a segunda porta, e assim por diante.

Por exemplo, `e0b` indica que uma porta Ethernet é a segunda porta na placa-mãe do nó.

As VLANs devem ser nomeadas usando a `port_name-vlan-id` sintaxe .

`port_name` especifica a porta física ou o grupo de interfaces.

`vlan-id` Especifica a identificação da VLAN na rede. Por exemplo, `e1c-80` é um nome de VLAN válido.

Configurar portas de rede

Combine portas físicas para criar grupos de interface

Um grupo de interface, também conhecido como Grupo de agregação de link (LAG), é criado combinando duas ou mais portas físicas no mesmo nó em uma única porta lógica. A porta lógica oferece maior resiliência, maior disponibilidade e compartilhamento de carga.

Tipos de grupo de interfaces

Três tipos de grupos de interface são suportados no sistema de armazenamento: Modo único, multimodo

estático e multimodo dinâmico. Cada grupo de interfaces fornece diferentes níveis de tolerância a falhas. Os grupos de interface multimodo fornecem métodos para o tráfego de rede de balanceamento de carga.

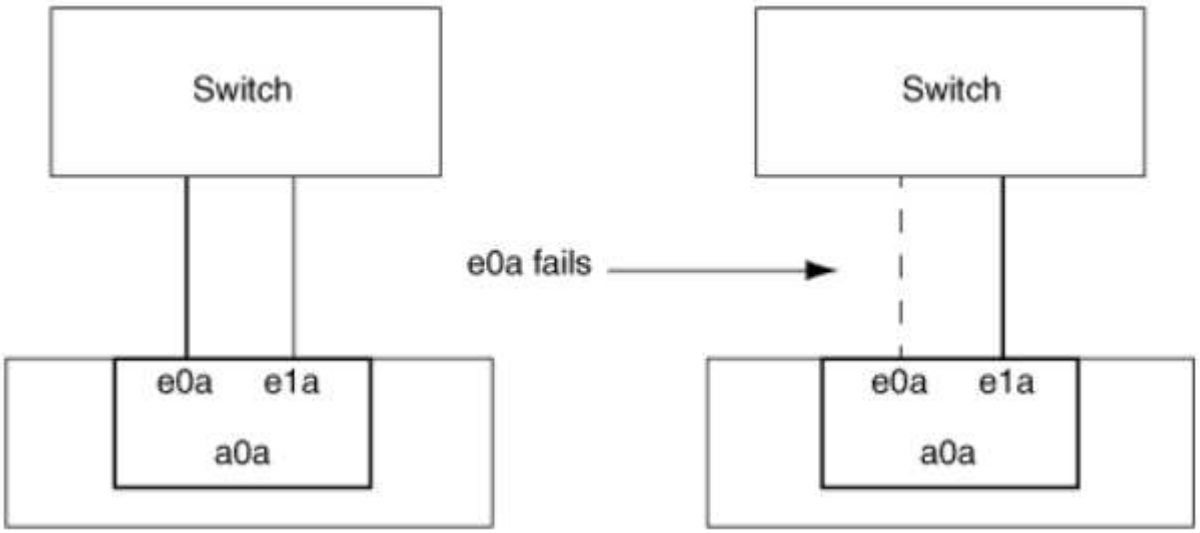
Caraterísticas dos grupos de interface monomodo

Em um grupo de interface de modo único, apenas uma das interfaces no grupo de interfaces está ativa. As outras interfaces estão em espera, prontas para assumir se a interface ativa falhar.

Caraterísticas de grupos de interface de modo único:

- Para failover, o cluster monitora o link ativo e controla o failover. Como o cluster monitora o link ativo, não há necessidade de configuração de switch.
- Pode haver mais de uma interface em espera em um grupo de interface de modo único.
- Se um grupo de interface de modo único abranger vários switches, você deve conetar os switches com um ISL (Inter-Switch Link).
- Para um grupo de interface de modo único, as portas do switch devem estar no mesmo domínio de broadcast.
- Os pacotes ARP de monitoramento de link, que têm um endereço de origem 0,0.0,0, são enviados pelas portas para verificar se as portas estão no mesmo domínio de broadcast.

A figura a seguir é um exemplo de um grupo de interface de modo único. Na figura, e0a e e1a fazem parte do grupo de interfaces monomodo a0a. Se a interface ativa, e0a, falhar, a interface standby e1a assume e mantém a conexão com o switch.



Para realizar a funcionalidade de modo único, a abordagem recomendada é usar grupos de failover. Ao usar um grupo de failover, a segunda porta ainda pode ser usada para outros LIFs e não precisa permanecer sem uso. Além disso, os grupos de failover podem abranger mais de duas portas e abranger portas em vários nós.

Caraterísticas de grupos de interface multimodo estático

A implementação do grupo de interfaces multimodo estático no ONTAP está em conformidade com a norma IEEE 802,3ad (estática). Qualquer switch que suporte agregados, mas não tenha troca de pacotes de controle para configurar um agregado, pode ser usado com grupos de interface multimodo estático.

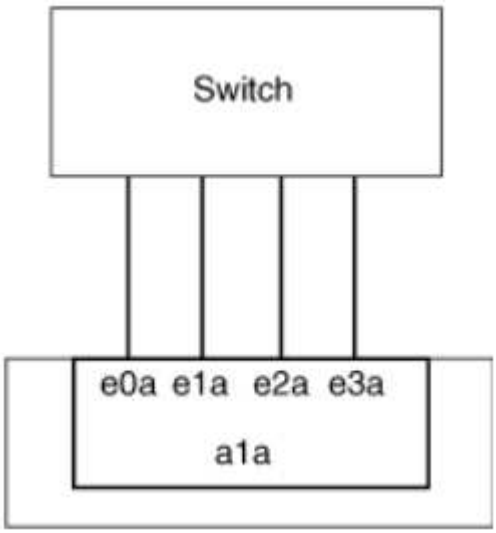
Os grupos de interface multimodo estático não estão em conformidade com a norma IEEE 802,3ad

(dinâmica), também conhecida como Link Aggregation Control Protocol (LACP). O LACP é equivalente ao Protocolo de agregação de portas (PAgP), o protocolo de agregação de links proprietário da Cisco.

A seguir estão as caraterísticas de um grupo de interfaces multimodo estático:

- Todas as interfaces do grupo de interfaces estão ativas e compartilham um único endereço MAC.
  - Várias conexões individuais são distribuídas entre as interfaces no grupo de interfaces.
  - Cada conexão ou sessão usa uma interface dentro do grupo de interfaces. Quando você usa o esquema de balanceamento de carga sequencial, todas as sessões são distribuídas por links disponíveis em uma base pacote a pacote e não são vinculadas a uma interface específica do grupo de interfaces.
- Grupos de interface multimodo estático podem se recuperar de uma falha de até interfaces "n-1", onde n é o número total de interfaces que formam o grupo de interfaces.
- Se uma porta falhar ou for desconetada, o tráfego que estava atravessando o link com falha será automaticamente redistribuído para uma das interfaces restantes.
- Os grupos de interface multimodo estático podem detetar uma perda de link, mas não conseguem detetar uma perda de conetividade com o cliente ou configurações incorretas de switch que possam afetar a conetividade e o desempenho.
- Um grupo de interface multimodo estático requer um switch que suporte a agregação de links em várias portas de switch. O switch é configurado de modo que todas as portas às quais os links de um grupo de interfaces estão conetados façam parte de uma única porta lógica. Alguns switches podem não suportar agregação de links de portas configuradas para quadros jumbo. Para obter mais informações, consulte a documentação do fornecedor do switch.
- Várias opções de balanceamento de carga estão disponíveis para distribuir o tráfego entre as interfaces de um grupo de interfaces multimodo estático.

A figura a seguir é um exemplo de um grupo de interfaces multimodo estático. As interfaces e0a, e1a, E2A e E3A fazem parte do grupo de interfaces multimodo A1A. Todas as quatro interfaces no grupo de interfaces multimodo A1A estão ativas.



Existem várias tecnologias que permitem que o tráfego em um único link agregado seja distribuído entre vários switches físicos. As tecnologias usadas para habilitar essa capacidade variam entre os produtos de rede. Os grupos de interface multimodo estático no ONTAP estão em conformidade com os padrões IEEE 802,3.3af. Se uma determinada tecnologia de agregação de links de múltiplos switches for considerada interoperacional ou conforme aos padrões IEEE 802,3.1X, ela deverá operar com o ONTAP.

O padrão IEEE 802,3 afirma que o dispositivo transmissor em um link agregado determina a interface física para transmissão. Portanto, o ONTAP é apenas responsável por distribuir tráfego de saída e não pode controlar como os quadros de entrada chegam. Se você quiser gerenciar ou controlar a transmissão de tráfego de entrada em um link agregado, essa transmissão deve ser modificada no dispositivo de rede conetado diretamente.

Grupo de interfaces multimodo dinâmico

Os grupos de interface multimodo dinâmico implementam o Link Aggregation Control Protocol (LACP) para comunicar a associação do grupo ao switch diretamente conetado. O LACP permite detetar a perda do status do link e a incapacidade do nó de se comunicar com a porta do switch de conexão direta.

A implementação dinâmica do grupo de interface multimodo no ONTAP está em conformidade com IEEE 802,3 AD (802,1 AX). O ONTAP não oferece suporte ao Protocolo de agregação de portas (PAgP), que é um protocolo de agregação de links proprietário da Cisco.

Um grupo de interface multimodo dinâmico requer um switch que suporte LACP.

O ONTAP implementa o LACP no modo ativo não configurável que funciona bem com switches configurados no modo ativo ou passivo. O ONTAP implementa os temporizadores LACP longos e curtos (para uso com valores não configuráveis de 3 segundos e 90 segundos), conforme especificado no IEEE 802,3 AD (802,1AX).

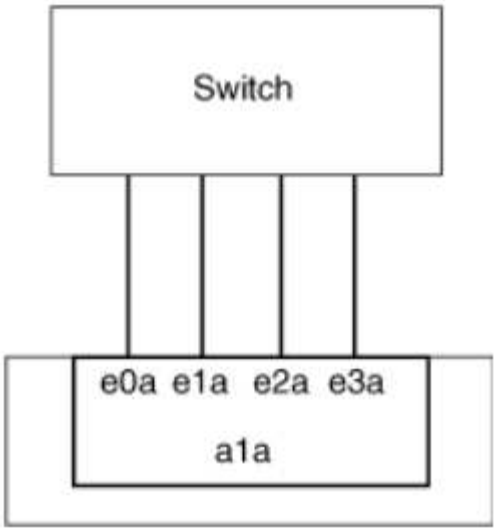
O algoritmo de balanceamento de carga do ONTAP determina a porta membro a ser usada para transmitir tráfego de saída e não controla como os quadros de entrada são recebidos. O switch determina o membro (porta física individual) de seu grupo de canais de portas a ser usado para transmissão, com base no algoritmo de balanceamento de carga configurado no grupo de canais de portas do switch. Portanto, a configuração do switch determina a porta membro (porta física individual) do sistema de armazenamento para receber tráfego. Para obter mais informações sobre como configurar o switch, consulte a documentação do fornecedor do switch.

Se uma interface individual não receber pacotes de protocolo LACP sucessivos, essa interface individual é marcada como "lag_inactive" na saída do comando "ifgrp status". O tráfego existente é automaticamente reencaminhado para quaisquer interfaces ativas restantes.

As regras a seguir se aplicam ao usar grupos de interface multimodo dinâmico:

- Os grupos de interface multimodo dinâmico devem ser configurados para usar os métodos de balanceamento de carga baseados em porta, baseados em IP, baseados em MAC ou round robin.
- Em um grupo de interface multimodo dinâmico, todas as interfaces devem estar ativas e compartilhar um único endereço MAC.

A figura a seguir é um exemplo de um grupo de interface multimodo dinâmico. As interfaces e0a, e1a, E2A e E3A fazem parte do grupo de interfaces multimodo A1A. Todas as quatro interfaces no grupo de interfaces multimodo dinâmico A1A estão ativas.



Balanceamento de carga em grupos de interface multimodo

Você pode garantir que todas as interfaces de um grupo de interfaces multimodo sejam igualmente utilizadas para o tráfego de saída usando o endereço IP, endereço MAC, métodos de balanceamento de carga sequenciais ou baseados em porta para distribuir o tráfego de rede igualmente pelas portas de rede de um grupo de interfaces multimodo.

O método de balanceamento de carga para um grupo de interfaces multimodo só pode ser especificado quando o grupo de interfaces é criado.

Prática recomendada: O balanceamento de carga baseado em porta é recomendado sempre que possível. Use balanceamento de carga baseado em porta, a menos que haja um motivo específico ou limitação na rede que o impeça.

Balanceamento de carga baseado em porta

O balanceamento de carga baseado em porta é o método recomendado.

Você pode equalizar o tráfego em um grupo de interfaces multimodo com base nas portas da camada de transporte (TCP/UDP) usando o método de balanceamento de carga baseado em porta.

O método de balanceamento de carga baseado em porta usa um algoritmo de hash rápido nos endereços IP de origem e destino, juntamente com o número da porta da camada de transporte.

Balanceamento de carga de endereço IP e endereço MAC

O balanceamento de carga de endereço IP e endereço MAC são os métodos para equalizar o tráfego em grupos de interface multimodo.

Esses métodos de balanceamento de carga usam um algoritmo de hash rápido nos endereços de origem e destino (endereço IP e endereço MAC). Se o resultado do algoritmo de hash mapear para uma interface que não está no estado de link UP, a próxima interface ativa será usada.

Não selecione o método de balanceamento de carga de endereço MAC ao criar grupos de interface em um sistema que se conete diretamente a um roteador. Em tal configuração, para cada quadro IP de saída, o endereço MAC de destino é o endereço MAC do roteador. Como resultado, apenas uma interface do grupo de interfaces é usada.

O balanceamento de carga de endereço IP funciona da mesma forma para endereços IPv4 e IPv6.

Balanceamento de carga sequencial

Você pode usar balanceamento de carga sequencial para distribuir pacotes de forma igual entre vários links usando um algoritmo round robin. Você pode usar a opção sequencial para balanceamento de carga do tráfego de uma única conexão em vários links para aumentar a taxa de transferência de conexão única.

No entanto, como o balanceamento de carga sequencial pode causar a entrega de pacotes fora do pedido, um desempenho extremamente ruim pode resultar. Portanto, o balanceamento de carga sequencial geralmente não é recomendado.

Crie um grupo de interfaces ou LAG

É possível criar um grupo de interfaces ou LAG (modo único, multimodo estático ou multimodo dinâmico (LACP) para apresentar uma única interface aos clientes combinando os recursos das portas de rede agregadas.

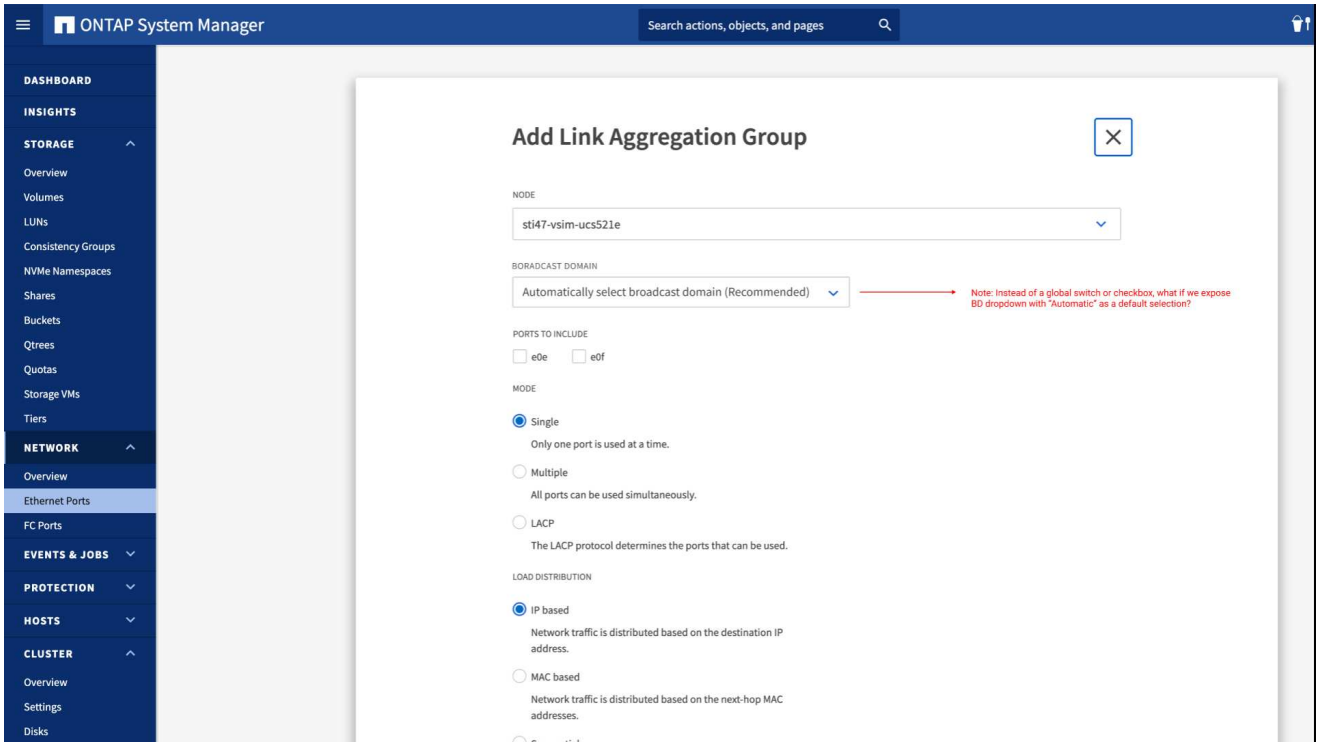
O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar um LAG

Passos

1. Selecione **rede > porta Ethernet > Grupo de agregação de link** para criar um LAG.
2. Selecione o nó na lista suspensa.
3. Escolha uma das seguintes opções:
   a. ONTAP para **selecionar automaticamente o domínio de transmissão (recomendado)**.
   b. Para selecionar manualmente um domínio de broadcast.
4. Selecione as portas para formar o LAG.
5. Selecione o modo:
   a. Único: Apenas uma porta é usada de cada vez.
   b. Múltiplas: Todas as portas podem ser usadas simultaneamente.
   c. LACP: O protocolo LACP determina as portas que podem ser usadas.
6. Selecione o balanceamento de carga:
   a. Baseado em IP
   b. Baseado em Mac
   c. Porta
   d. Sequencial
7. Salve suas alterações.



CLI

Use a CLI para criar um grupo de interfaces

Para obter uma lista completa de restrições de configuração aplicáveis a grupos de interface de portas, consulte a `network port ifgrp add-port` página de manual.

Ao criar um grupo de interfaces multimodo, você pode especificar qualquer um dos seguintes métodos de balanceamento de carga:

- `port`: O tráfego de rede é distribuído com base nas portas da camada de transporte (TCP/UDP). Este é o método de balanceamento de carga recomendado.
- `mac`: O tráfego de rede é distribuído com base em endereços MAC.
- `ip`: O tráfego de rede é distribuído com base em endereços IP.
- `sequential`: O tráfego de rede é distribuído à medida que é recebido.

> O endereço MAC de um grupo de interfaces é determinado pela ordem das portas subjacentes e como essas portas são inicializadas durante a inicialização. Portanto, você não deve assumir que o endereço MAC do ifgrp é persistente em reinicializações ou atualizações do ONTAP.

Passo

Use o `network port ifgrp create` comando para criar um grupo de interfaces.

Os grupos de interface devem ser nomeados usando a `a<number><letter>` sintaxe . Por exemplo, a0a, a0b, A1c e A2A são nomes de grupos de interface válidos.

Para obter mais informações sobre esse comando, consulte "Referência do comando ONTAP" .

O exemplo a seguir mostra como criar um grupo de interfaces chamado a0a com uma função de distribuição de porta e um modo de multimodo:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

Adicione uma porta a um grupo de interfaces ou LAG

Você pode adicionar até 16 portas físicas a um grupo de interfaces ou LAG para todas as velocidades de portas.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para adicionar uma porta a um LAG

Passos

1. Selecione **rede > porta Ethernet > LAG** para editar um LAG.
2. Selecione portas adicionais no mesmo nó para adicionar ao LAG.
3. Salve suas alterações.

CLI

Use a CLI para adicionar portas a um grupo de interfaces

Passo

Adicionar portas de rede ao grupo de interfaces:

```
network port ifgrp add-port
```

Para obter mais informações sobre esse comando, consulte "Referência do comando ONTAP" .

O exemplo a seguir mostra como adicionar a porta e0c a um grupo de interfaces chamado a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

A partir do ONTAP 9.8, os grupos de interface são automaticamente colocados em um domínio de broadcast apropriado cerca de um minuto após a primeira porta física ser adicionada ao grupo de interfaces. Se você não quiser que o ONTAP faça isso e preferir colocar manualmente o ifgrp em um domínio de broadcast, especifique o `-skip-broadcast-domain-placement` parâmetro como parte do `ifgrp add-port` comando.

Remova uma porta de um grupo de interfaces ou LAG

Você pode remover uma porta de um grupo de interfaces que hospeda LIFs, desde que não seja a última porta no grupo de interfaces. Não há nenhum requisito de que o grupo de interfaces não deve hospedar LIFs ou que o grupo de interfaces não deve ser a porta inicial de um LIF, considerando que você não está removendo a última porta do grupo de interfaces. No entanto, se você estiver removendo a última porta, então você deve migrar ou mover os LIFs do grupo de interfaces primeiro.

Sobre esta tarefa

Você pode remover até 16 portas (interfaces físicas) de um grupo de interfaces ou LAG.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para remover uma porta de um LAG

Passos

1. Selecione **rede > porta Ethernet > LAG** para editar um LAG.
2. Selecione as portas a serem removidas do LAG.
3. Salve suas alterações.

CLI

Use a CLI para remover portas de um grupo de interfaces

Passo

Remover portas de rede de um grupo de interfaces:

```
network port ifgrp remove-port
```

O exemplo a seguir mostra como remover a porta e0c de um grupo de interfaces chamado a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Exclua um grupo de interfaces ou LAG

Você pode excluir grupos de interface ou LAGs se quiser configurar LIFs diretamente nas portas físicas subjacentes ou decidir alterar o grupo de interfaces ou o modo LAG ou a função de distribuição.

Antes de começar

- O grupo de interfaces ou LAG não deve estar hospedando um LIF.
- O grupo de interfaces ou LAG não deve ser nem a porta inicial nem o destino de failover de um LIF.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para excluir um LAG

Passos

1. Selecione **rede > porta Ethernet > LAG** para excluir um LAG.
2. Selecione o LAG que deseja remover.
3. Eliminar o LAG.

CLI

Use a CLI para excluir um grupo de interfaces

Passo

Use o `network port ifgrp delete` comando para excluir um grupo de interfaces.

Para obter mais informações sobre esse comando, consulte "Referência do comando ONTAP" .

O exemplo a seguir mostra como excluir um grupo de interfaces chamado a0b:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Configurar VLANs em portas físicas

Você pode usar VLANs no ONTAP para fornecer segmentação lógica de redes, criando domínios de broadcast separados que são definidos em uma base de porta de switch, em vez dos domínios de broadcast tradicionais, definidos em limites físicos.

Uma VLAN pode abranger vários segmentos físicos de rede. As estações finais pertencentes a uma VLAN estão relacionadas por função ou aplicação.

Por exemplo, as estações finais em uma VLAN podem ser agrupadas por departamentos, como engenharia e contabilidade, ou por projetos, como release1 e release2. Como a proximidade física das estações finais não é essencial em uma VLAN, você pode dispersar as estações finais geograficamente e ainda conter o domínio de broadcast em uma rede comutada.

No ONTAP 9.13,1 e no 9.14.1, as portas não marcadas que não são utilizadas por quaisquer interfaces lógicas (LIFs) e não têm conetividade VLAN nativa no switch conetado são marcadas como degradadas. Isso ajuda a identificar portas não utilizadas e não indica uma interrupção. As VLANs nativas permitem tráfego não marcado na porta base ifgrp, como transmissões ONTAP CFM. Configure VLANs nativas no switch para evitar o bloqueio de tráfego não marcado.

Você pode gerenciar VLANs criando, excluindo ou exibindo informações sobre elas.

> Você não deve criar uma VLAN em uma interface de rede com o mesmo identificador que a VLAN nativa do switch. Por exemplo, se a interface de rede e0b estiver na VLAN 10 nativa, você não deverá criar uma VLAN e0b-10 nessa interface.

Crie uma VLAN

Você pode criar uma VLAN para manter domínios de broadcast separados dentro do mesmo domínio de rede usando o System Manager ou o `network port vlan create` comando.

Antes de começar

Confirme se os seguintes requisitos foram cumpridos:

- Os switches implantados na rede devem estar em conformidade com os padrões IEEE 802,1Q.1X ou ter uma implementação de VLANs específica do fornecedor.
- Para suportar várias VLANs, uma estação final deve ser estaticamente configurada para pertencer a uma ou mais VLANs.
- A VLAN não está conetada a uma porta que hospeda um LIF de cluster.
- A VLAN não está conetada às portas atribuídas ao IPspace do cluster.
- A VLAN não é criada em uma porta de grupo de interfaces que não contém portas membro.

Sobre esta tarefa

A criação de uma VLAN coneta a VLAN à porta de rede em um nó especificado em um cluster.

Quando você configura uma VLAN por uma porta pela primeira vez, a porta pode cair, resultando em uma desconexão temporária da rede. As adições subsequentes de VLAN à mesma porta não afetam o estado da porta.

> Você não deve criar uma VLAN em uma interface de rede com o mesmo identificador que a VLAN nativa do switch. Por exemplo, se a interface de rede e0b estiver na VLAN 10 nativa, você não deverá criar uma VLAN e0b-10 nessa interface.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar uma VLAN

A partir do ONTAP 9.12,0, pode selecionar automaticamente o domínio de difusão ou selecionar manualmente ligado na lista. Anteriormente, os domínios de broadcast eram sempre selecionados automaticamente com base na conetividade da camada 2. Se você selecionar manualmente um domínio de broadcast, um aviso será exibido indicando que selecionar manualmente um domínio de broadcast pode resultar em perda de conetividade.

Passos

1. Selecione **rede > porta Ethernet > VLAN**.
2. Selecione o nó na lista suspensa.
3. Escolha uma das seguintes opções:
   a. ONTAP para **selecionar automaticamente o domínio de transmissão (recomendado)**.
   b. Para selecionar manualmente um domínio de broadcast na lista.
4. Selecione as portas para formar a VLAN.
5. Especifique o ID da VLAN.
6. Salve suas alterações.

CLI

Use a CLI para criar uma VLAN

Em certas circunstâncias, se você quiser criar a porta VLAN em uma porta degradada sem corrigir o problema de hardware ou qualquer configuração incorreta de software, então você pode definir o `-ignore-health-status` parâmetro `network port modify` do comando como `true`.

Passos

1. Use o `network port vlan create` comando para criar uma VLAN.
2. Você deve especificar `vlan-name` as opções ou `port` e `vlan-id` ao criar uma VLAN. O nome da VLAN é uma combinação do nome da porta (ou grupo de interfaces) e do identificador VLAN do switch de rede, com um hífen entre. Por exemplo, `e0c-24` e `e1c-80` são nomes de VLAN válidos.

O exemplo a seguir mostra como criar uma VLAN `e1c-80` conetada à porta de rede `e1c` no nó `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

A partir do ONTAP 9.8, as VLANs são automaticamente colocadas em domínios de broadcast apropriados cerca de um minuto após sua criação. Se você não quiser que o ONTAP faça isso e preferir colocar manualmente a VLAN em um domínio de broadcast, especifique o `-skip-broadcast-domain-placement` parâmetro como parte do `vlan create` comando.

Para obter mais informações sobre esse comando, consulte "Referência do comando ONTAP" .

Editar uma VLAN

Você pode alterar o domínio de broadcast ou desativar uma VLAN.

Use o System Manager para editar uma VLAN

A partir do ONTAP 9.12,0, pode selecionar automaticamente o domínio de difusão ou selecionar manualmente ligado na lista. Os domínios de broadcast anteriormente eram sempre selecionados automaticamente com base na conetividade da camada 2. Se você selecionar manualmente um domínio de broadcast, um aviso será exibido indicando que selecionar manualmente um domínio de broadcast pode resultar em perda de conetividade.

Passos

1. Selecione **rede > porta Ethernet > VLAN**.
2. Selecione o ícone de edição.
3. Execute um dos seguintes procedimentos:
   - Altere o domínio de broadcast selecionando um outro da lista.
   - Desmarque a caixa de seleção **Enabled** (habilitado).
4. Salve suas alterações.

Eliminar um VLAN

Talvez seja necessário excluir uma VLAN antes de remover uma NIC do slot. Quando você exclui uma VLAN, ela é automaticamente removida de todas as regras de failover e grupos que a usam.

Antes de começar

Certifique-se de que não existem LIFs associados à VLAN.

Sobre esta tarefa

A exclusão da última VLAN de uma porta pode causar uma desconexão temporária da rede da porta.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para excluir uma VLAN

Passos

1. Selecione **rede > porta Ethernet > VLAN**.
2. Selecione a VLAN que deseja remover.
3. Clique em **Excluir**.

CLI

Use a CLI para excluir uma VLAN

Passo

Use o `network port vlan delete` comando para excluir uma VLAN.

O exemplo a seguir mostra como excluir VLAN `e1c-80` da porta de rede `e1c` no nó `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

Modificar atributos de porta de rede

Você pode modificar as configurações de negociação automática, duplex, controle de fluxo, velocidade e integridade de uma porta de rede física.

Antes de começar

A porta que você deseja modificar não deve estar hospedando nenhum LIFs.

Sobre esta tarefa

- Não é recomendável modificar as configurações administrativas das interfaces de rede de 100 GbE, 40 GbE, 10 GbE ou 1 GbE.

  Os valores definidos para o modo duplex e a velocidade da porta são referidos como definições administrativas. Dependendo das limitações da rede, as configurações administrativas podem diferir das configurações operacionais (ou seja, o modo duplex e a velocidade que a porta realmente usa).

- Não é recomendável modificar as configurações administrativas das portas físicas subjacentes em um grupo de interfaces.

  O `-up-admin` parâmetro (disponível no nível de privilégio avançado) modifica as definições administrativas da porta.

- Não é recomendável definir a `-up-admin` configuração administrativa como falsa para todas as portas em um nó ou para a porta que hospeda o último LIF de cluster operacional em um nó.
- Não é recomendável modificar o tamanho da MTU da porta de gerenciamento, `e0M`.
- O tamanho da MTU de uma porta em um domínio de broadcast não pode ser alterado do valor MTU definido para o domínio de broadcast.
- O tamanho da MTU de uma VLAN não pode exceder o valor do tamanho da MTU de sua porta base.

Passos

1. Modifique os atributos de uma porta de rede:

   `network port modify`

2. Você pode definir o `-ignore-health-status` campo como verdadeiro para especificar que o sistema pode ignorar o status de integridade da porta de rede de uma porta especificada.

   O status de integridade da porta de rede é alterado automaticamente de degradada para saudável, e essa porta agora pode ser usada para hospedar LIFs. Você deve definir o controle de fluxo das portas do cluster como `none`. Por padrão, o controle de fluxo é definido como `full`.

O comando a seguir desativa o controle de fluxo na porta e0b definindo o controle de fluxo como nenhum:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

Converta 40GbE portas NIC em várias portas 10GbE para conetividade 10GbE

Pode converter as placas de interface de rede (NICs) X1144A-R6 e X91440A-R6 40GbE para suportar quatro portas 10GbE.

Se você estiver conetando uma plataforma de hardware que suporte uma dessas NICs a um cluster que suporte a interconexão de cluster 10GbE e conexões de dados do cliente, a NIC deve ser convertida para fornecer as conexões 10GbE necessárias.

Antes de começar

Você deve estar usando um cabo multicondutor suportado.

Sobre esta tarefa

Para obter uma lista completa de plataformas que suportam NICs, consulte "Hardware Universe" .

> Na NIC X1144A-R6, somente a porta A pode ser convertida para suportar as quatro conexões 10GbE. Uma vez que a porta A é convertida, a porta e não está disponível para uso.

Passos

1. Entre no modo de manutenção.
2. Converta a NIC do suporte 40GbE para o suporte 10GbE.

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. Depois de usar o comando Convert, interrompa o nó.
4. Instale ou substitua o cabo.
5. Dependendo do modelo de hardware, use o SP (processador de serviço) ou o BMC (controlador de gerenciamento de placa base) para ligar o nó para que a conversão entre em vigor.

Configure as portas UTA X1143A-R6 para o seu sistema ONTAP

Por padrão, o adaptador de destino unificado X1143A-R6 é configurado no modo de destino FC, mas você pode configurar suas portas como portas Ethernet de 10 GB e FCoE (CNA) ou como portas de iniciador FC de 16 GB ou de destino. Isso requer adaptadores SFP diferentes.

Quando configurados para Ethernet e FCoE, os adaptadores X1143A-R6 suportam NIC concorrente e tráfego de destino FCoE na mesma porta de 10 GBE. Quando configurado para FC, cada par de duas portas que compartilha o mesmo ASIC pode ser configurado individualmente para o modo de iniciador FC ou destino. Isso significa que um único adaptador X1143A-R6 pode oferecer suporte ao modo de destino FC em um par de duas portas e no modo iniciador FC em outro par de duas portas. Os pares de portas ligados ao mesmo ASIC têm de ser configurados no mesmo modo.

No modo FC, o adaptador X1143A-R6 se comporta como qualquer dispositivo FC existente com velocidades de até 16 Gbps. No modo CNA, você pode usar o adaptador X1143A-R6 para NIC concorrente e compartilhamento de tráfego FCoE na mesma porta de 10 GbE. O modo CNA só suporta o modo de destino FC para a função FCoE.

Para configurar o adaptador de destino unificado (X1143A-R6), você deve configurar as duas portas adjacentes no mesmo chip no mesmo modo de personalidade.

Passos

1. Veja a configuração da porta:

```
system hardware unified-connect show
```

2. Configure as portas conforme necessário para Fibre Channel (FC) ou adaptador de rede convergente (CNA):

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. Conete os cabos apropriados para FC ou Ethernet de 10 GB.
4. Verifique se você tem o SFP correto instalado:

```
network fcp adapter show -instance -node -adapter
```

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB, com base na malha FC conetada.

Esconda o porto UTA2 em ONTAP

Pode converter a porta UTA2 do modo de adaptador de rede convergente (CNA) para o modo Fibre Channel (FC) ou vice-versa.

Você deve alterar a personalidade UTA2 do modo CNA para o modo FC quando precisar alterar o meio físico

que coneta a porta à sua rede ou para suportar os iniciadores e o destino FC.

Do modo CNA para o modo FC

Passos

1. Coloque o adaptador offline:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Alterar o modo de porta:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. Reinicie o nó e, em seguida, coloque o adaptador online:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. Notifique seu administrador ou gerenciador de VIF para excluir ou remover a porta, conforme aplicável:
   - Se a porta for usada como uma porta inicial de um LIF, for um membro de um grupo de interfaces (ifgrp) ou hosts VLANs, então um administrador deve fazer o seguinte:
     - Mova os LIFs, remova a porta do ifgrp ou exclua as VLANs, respetivamente.
     - Exclua manualmente a porta executando o `network port delete` comando. Se o `network port delete` comando falhar, o administrador deve resolver os erros e, em seguida, executar o comando novamente.
   - Se a porta não for usada como porta inicial de um LIF, não for membro de um ifgrp e não hospedar VLANs, o gerenciador de VIF deve remover a porta de seus Registros no momento da reinicialização. Se o gerenciador de VIF não remover a porta, o administrador deve removê-la manualmente após a reinicialização usando o `network port delete` comando.
5. Verifique se você tem o SFP correto instalado:

```
network fcp adapter show -instance -node -adapter
```

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB antes de alterar a configuração no nó.

Do modo FC para o modo CNA

Passos

1. Coloque o adaptador offline:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Alterar o modo de porta:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. Reinicie o nó
4. Verifique se você tem o SFP correto instalado.

   Para CNA, você deve usar um SFP Ethernet 10Gb.

Converta os módulos óticos CNA/UTA2 para o seu sistema ONTAP

Você deve alterar os módulos óticos no adaptador de destino unificado (CNA/UTA2) para suportar o modo de personalidade que você selecionou para o adaptador.

Passos

1. Verifique o SFP atual usado na placa. Em seguida, substitua o SFP atual pelo SFP apropriado para a personalidade preferida (FC ou CNA).
2. Remova os módulos óticos atuais do adaptador X1143A-R6.
3. Insira os módulos corretos para a ótica do seu modo de personalidade (FC ou CNA) preferido.
4. Verifique se você tem o SFP correto instalado:

```
network fcp adapter show -instance -node -adapter
```

   Os módulos SFP mais suportados e os cabos de cobre (Twinax) da marca Cisco estão listados na "NetApp Hardware Universe".

Removendo uma NIC do nó (ONTAP 9.8 e posterior)

Este tópico aplica-se ao ONTAP 9.8 e posterior. Você pode ter que remover uma NIC defeituosa de seu slot ou mover a NIC para outro slot para fins de manutenção.

Passos

1. Desligue o nó.
2. Remova fisicamente a NIC do respetivo slot.
3. Ligue o nó.
4. Verifique se a porta foi excluída:

```
network port show
```

O ONTAP remove automaticamente a porta de qualquer grupo de interface. Se a porta fosse o único membro de um grupo de interfaces, o grupo de interfaces será excluído.

5. Se a porta tiver quaisquer VLANs configuradas, elas serão deslocadas. Você pode exibir VLANs deslocadas usando o seguinte comando:

```
cluster controller-replacement network displaced-vlans show
```

Os `displaced-interface show` comandos , `displaced-vlans show`, e `displaced-vlans restore` são únicos e não requerem o nome do comando totalmente qualificado, que começa com `cluster controller-replacement network`.

6. Essas VLANs são excluídas, mas podem ser restauradas usando o seguinte comando:

```
displaced-vlans restore
```

7. Se a porta tivesse quaisquer LIFs configuradas nela, o ONTAP escolherá automaticamente novas portas residenciais para esses LIFs em outra porta no mesmo domínio de broadcast. Se nenhuma porta inicial adequada for encontrada no mesmo arquivador, esses LIFs são considerados deslocados. Você pode visualizar LIFs deslocados usando o seguinte comando:

   `displaced-interface show`

8. Quando uma nova porta é adicionada ao domínio de broadcast no mesmo nó, as portas iniciais para os LIFs são restauradas automaticamente. Alternativamente, você pode definir a porta inicial usando `network interface modify -home-port -home-node or use the displaced- interface restore` o comando.

Removendo uma NIC do nó (ONTAP 9.7 ou anterior)

Este tópico aplica-se ao ONTAP 9.7 ou anterior. Você pode ter que remover uma NIC defeituosa de seu slot ou mover a NIC para outro slot para fins de manutenção.

Antes de começar

- Todos os LIFs hospedados nas portas NIC devem ter sido migrados ou excluídos.
- Nenhuma das portas NIC pode ser a porta inicial de quaisquer LIFs.
- Você deve ter Privileges avançado para excluir as portas de uma NIC.

Passos

1. Exclua as portas da NIC:

   `network port delete`

2. Verifique se as portas foram excluídas:

   `network port show`

3. Repita a etapa 1, se a saída do comando network port show ainda exibir a porta excluída.

Monitorar portas de rede

Monitore a integridade das portas de rede

O gerenciamento ONTAP de portas de rede inclui monitoramento automático de integridade e um conjunto de monitores de integridade para ajudá-lo a identificar portas de rede que podem não ser adequadas para hospedar LIFs.

Sobre esta tarefa

Se um monitor de integridade determinar que uma porta de rede não está saudável, ele avisa os administradores por meio de uma mensagem EMS ou marca a porta como degradada. O ONTAP evita hospedar LIFs em portas de rede degradadas se houver destinos de failover alternativos saudáveis para esse LIF. Uma porta pode se degradar devido a um evento de falha suave, como flapping de link (links que saltam rapidamente entre cima e baixo) ou particionamento de rede:

- As portas de rede no IPspace do cluster são marcadas como degradadas quando apresentam flapping de link ou perda de acessibilidade da camada 2 (L2) a outras portas de rede no domínio de broadcast.
- As portas de rede em IPspaces que não sejam de cluster são marcadas como degradadas quando apresentam flapping de link.

Você deve estar ciente dos seguintes comportamentos de uma porta degradada:

- Uma porta degradada não pode ser incluída em uma VLAN ou em um grupo de interfaces.

  Se uma porta membro de um grupo de interfaces for marcada como degradada, mas o grupo de interfaces ainda estiver marcado como saudável, LIFs podem ser hospedados nesse grupo de interfaces.

- Os LIFs são migrados automaticamente de portas degradadas para portas íntegras.
- Durante um evento de failover, uma porta degradada não é considerada como o destino de failover. Se não houver portas íntegras disponíveis, as portas degradadas hospedam LIFs de acordo com a política de failover normal.
- Não é possível criar, migrar ou reverter um LIF para uma porta degradada.

  Pode modificar a `ignore-health-status` definição da porta de rede para `true`. Em seguida, você pode hospedar um LIF nas portas saudáveis.

Passos

1. Inicie sessão no modo de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Verifique quais monitores de integridade estão ativados para monitorar o estado da porta de rede:

   ```
   network options port-health-monitor show
   ```

   O status de integridade de uma porta é determinado pelo valor dos monitores de integridade.

Os seguintes monitores de integridade estão disponíveis e ativados por padrão no ONTAP:

- Monitor de saúde com link flapping: Monitora o flapping do link

  Se uma porta tiver um link batendo mais de uma vez em cinco minutos, essa porta será marcada como degradada.

- Monitor de integridade de acessibilidade L2: Monitora se todas as portas configuradas no mesmo domínio de broadcast têm acessibilidade L2

  Esse monitor de integridade relata L2 problemas de acessibilidade em todos os IPspaces; no entanto, ele marca apenas as portas no IPspace do cluster como degradadas.

- Monitor CRC: Monitora as estatísticas de CRC nas portas

  Este monitor de integridade não marca uma porta como degradada, mas gera uma mensagem EMS quando se observa uma taxa de falha de CRC muito alta.

3. Ative ou desative qualquer um dos monitores de integridade para um espaço IPspace conforme desejado usando o `network options port-health-monitor modify` comando.
4. Veja a integridade detalhada de um porto:

```
network port show -health
```

O comando output exibe o status de integridade da porta, `ignore health status` configuração e lista dos motivos pelos quais a porta é marcada como degradada.

Um status de integridade da porta pode ser `healthy` ou `degraded`.

Se a `ignore health status` configuração for `true`, ela indica que o status de integridade da porta foi modificado de `degraded` para `healthy` pelo administrador.

Se a `ignore health status` configuração for `false`, o status de integridade da porta será determinado automaticamente pelo sistema.

Monitorar a acessibilidade das portas de rede (ONTAP 9.8 e posterior)

O monitoramento de acessibilidade é integrado ao ONTAP 9.8 e posterior. Use esse monitoramento para identificar quando a topologia de rede física não corresponde à configuração do ONTAP. Em alguns casos, o ONTAP pode reparar a acessibilidade da porta. Em outros casos, etapas adicionais são necessárias.

Sobre esta tarefa

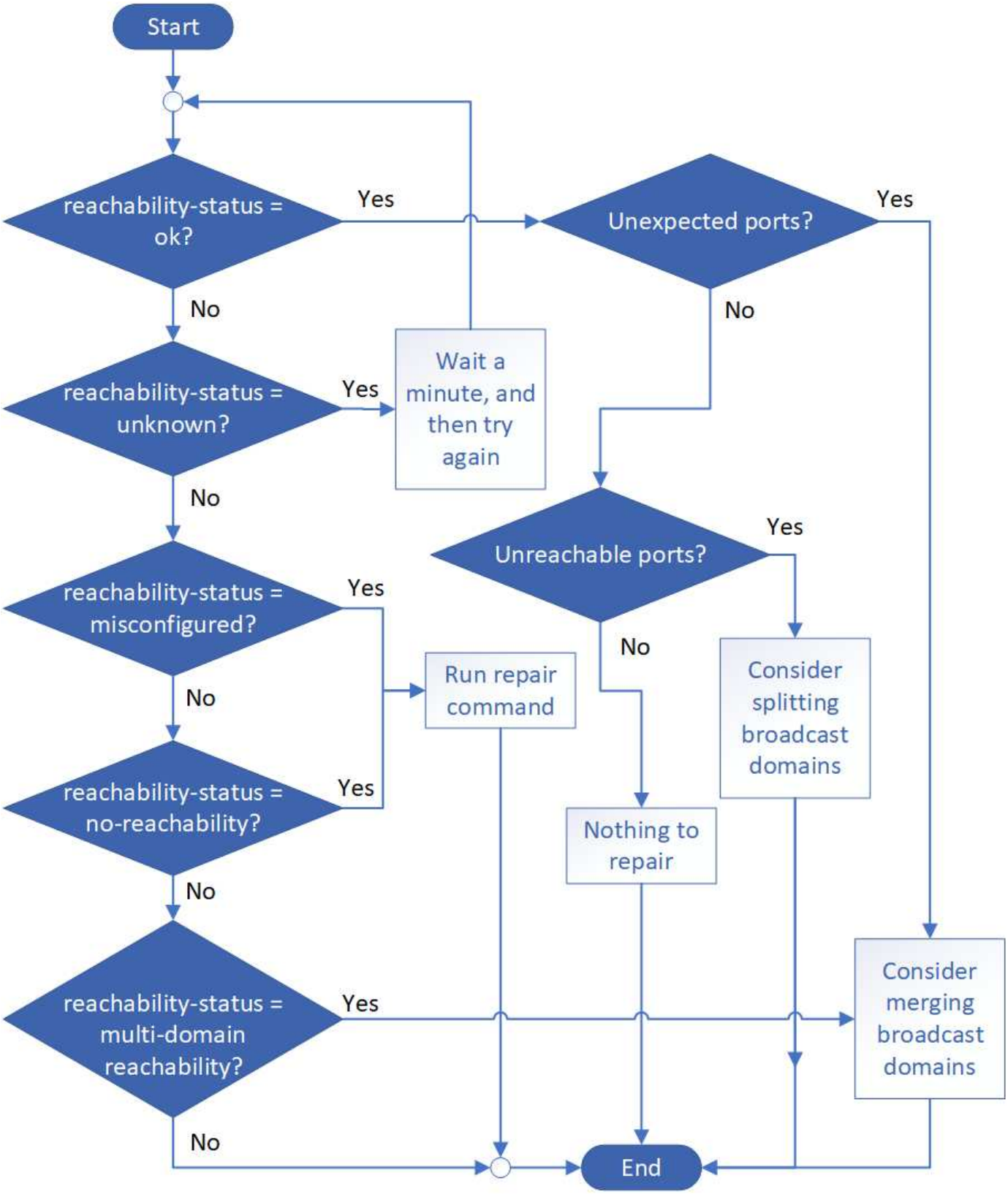
Use esses comandos para verificar, diagnosticar e reparar configurações incorretas de rede resultantes da configuração do ONTAP que não corresponde ao cabeamento físico ou à configuração do switch de rede.

Passo

1. Exibir acessibilidade da porta:

```
network port reachability show
```

2. Use a seguinte árvore de decisão e tabela para determinar a próxima etapa, se houver.



Status de acessibilidade	Descrição
ok	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído. Se o status de acessibilidade for "ok", mas houver "portas inesperadas", considere mesclar um ou mais domínios de broadcast. Para obter mais informações, consulte a seguinte linha *portas inesperadas*. Se o status de acessibilidade for "ok", mas houver "portas inalcançáveis", considere dividir um ou mais domínios de broadcast. Para obter mais informações, consulte a seguinte linha *portas inalcançáveis*. Se o status de acessibilidade for "ok" e não houver portas inesperadas ou inacessíveis, sua configuração está correta.
Portas inesperadas	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast. Examine a conetividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast. Para obter mais informações, "Mesclar domínios de broadcast"consulte .
Portas inalcançáveis	Se um único domínio de broadcast tiver sido particionado em dois conjuntos de acessibilidade diferentes, você poderá dividir um domínio de broadcast para sincronizar a configuração do ONTAP com a topologia de rede física. Normalmente, a lista de portas inalcançáveis define o conjunto de portas que devem ser divididas em outro domínio de broadcast depois de ter verificado que a configuração física e do switch é precisa. Para obter mais informações, "Dividir domínios de broadcast"consulte .
acessibilidade mal configurada	A porta não tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, a porta tem acessibilidade da camada 2 para um domínio de broadcast diferente. Você pode reparar a acessibilidade da porta. Ao executar o seguinte comando, o sistema atribuirá a porta ao domínio de broadcast ao qual tem acessibilidade: `network port reachability repair -node -port` Para obter mais informações, "Acessibilidade da porta de reparo"consulte .

sem acessibilidade	A porta não tem acessibilidade da camada 2 para qualquer domínio de broadcast existente. Você pode reparar a acessibilidade da porta. Quando você executa o seguinte comando, o sistema atribuirá a porta a um novo domínio de broadcast criado automaticamente no IPspace padrão: `network port reachability repair -node -port` Para obter mais informações, "Acessibilidade da porta de reparo"consulte .
multidomínio-acessibilidade	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast. Examine a conetividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast. Para obter mais informações, consulte "Mesclar domínios de broadcast" ou "Acessibilidade da porta de reparo".
desconhecido	Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.

Depois de reparar uma porta, você precisa verificar e resolver LIFs e VLANs deslocados. Se a porta fazia parte de um grupo de interfaces, você também precisa entender o que aconteceu com esse grupo de interfaces. Para obter mais informações, "Acessibilidade da porta de reparo"consulte .

Visão geral das portas ONTAP

Várias portas conhecidas são reservadas para comunicações ONTAP com serviços específicos. Conflitos de portas ocorrerão se um valor de porta no ambiente de rede de storage for o mesmo que na porta ONTAP.

A tabela a seguir lista as portas TCP e UDP usadas pelo ONTAP.

Serviço	Porta/protocolo	Descrição
ssh	22/TCP	Login de shell seguro
telnet	23/TCP	Início de sessão remoto
DNS	53/TCP	Carregue o DNS balanceado
http	80/TCP	Protocolo de transferência de texto Hyper
rpcbind	111/TCP	Chamada de procedimento remoto
rpcbind	111/UDP	Chamada de procedimento remoto
ntp	123/UDP	Protocolo de hora de rede
msrpc	135/UDP	MSRPC
netbios-ssn	139/TCP	Sessão de serviço NetBIOS

snmp	161/UDP	Protocolo de gerenciamento de rede simples
https	443/TCP	HTTP em TLS
microsoft-ds	445/TCP	Microsoft-ds
montagem	635/TCP	Montagem em NFS
montagem	635/UDP	Suporte NFS
nomeado	953/UDP	Daemon de nomes
nfs	2049/UDP	Daemon do servidor NFS
nfs	2049/TCP	Daemon do servidor NFS
nrv	2050/TCP	Protocolo de volume remoto da NetApp
iscsi	3260/TCP	Porta de destino iSCSI
lockd	4045/TCP	Daemon de bloqueio NFS
lockd	4045/UDP	Daemon de bloqueio NFS
NSM	4046/TCP	Monitor de estado da rede
NSM	4046/UDP	Monitor de estado da rede
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS - protocolo binário de escuta
https	8443/TCP	Ferramenta GUI 7MTT através de https
ndmp	10000/TCP	Protocolo de gerenciamento de dados de rede
Peering de clusters	11104/TCP	Peering de cluster, bidirecional
Peering de cluster, bidirecional	11105/TCP	Peering de clusters
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	aceite as ligações de controlo através de tomadas seguras
porta de testemunhas cifs	40001/TCP	porta de testemunhas cifs
tls	50000/TCP	Segurança da camada de transporte
iscsi	65200/TCP	Porta de ISCSI

Portas internas do ONTAP

A tabela a seguir lista as portas TCP e UDP que são usadas internamente pelo ONTAP. Essas portas são usadas para estabelecer comunicação LIF entre clusters:

Porta/protocolo	Descrição
514	Syslog

900	RPC de cluster do NetApp
902	RPC de cluster do NetApp
904	RPC de cluster do NetApp
905	RPC de cluster do NetApp
910	RPC de cluster do NetApp
911	RPC de cluster do NetApp
913	RPC de cluster do NetApp
914	RPC de cluster do NetApp
915	RPC de cluster do NetApp
918	RPC de cluster do NetApp
920	RPC de cluster do NetApp
921	RPC de cluster do NetApp
924	RPC de cluster do NetApp
925	RPC de cluster do NetApp
927	RPC de cluster do NetApp
928	RPC de cluster do NetApp
929	RPC de cluster do NetApp
931	RPC de cluster do NetApp
932	RPC de cluster do NetApp
933	RPC de cluster do NetApp
934	RPC de cluster do NetApp
935	RPC de cluster do NetApp
936	RPC de cluster do NetApp
937	RPC de cluster do NetApp
939	RPC de cluster do NetApp
940	RPC de cluster do NetApp
951	RPC de cluster do NetApp
954	RPC de cluster do NetApp
955	RPC de cluster do NetApp
956	RPC de cluster do NetApp
958	RPC de cluster do NetApp
961	RPC de cluster do NetApp
963	RPC de cluster do NetApp
964	RPC de cluster do NetApp

966	RPC de cluster do NetApp
967	RPC de cluster do NetApp
982	RPC de cluster do NetApp
983	RPC de cluster do NetApp
5125	Porta de controle alternativa para disco
5133	Porta de controle alternativa para disco
5144	Porta de controle alternativa para disco
65502	Escopo do nó SSH
65503	Compartilhamento de LIF
7810	RPC de cluster do NetApp
7811	RPC de cluster do NetApp
7812	RPC de cluster do NetApp
7813	RPC de cluster do NetApp
7814	RPC de cluster do NetApp
7815	RPC de cluster do NetApp
7816	RPC de cluster do NetApp
7817	RPC de cluster do NetApp
7818	RPC de cluster do NetApp
7819	RPC de cluster do NetApp
7820	RPC de cluster do NetApp
7821	RPC de cluster do NetApp
7822	RPC de cluster do NetApp
7823	RPC de cluster do NetApp
7824	RPC de cluster do NetApp
8023	Escopo do nó TELNET
8514	RSH do âmbito do nó
9877	Porta do cliente KMIP (somente host local interno)

IPspaces

Configurar a visão geral dos IPspaces

Os IPspaces permitem configurar um único cluster ONTAP para que ele possa ser acessado por clientes de mais de um domínio de rede administrativamente separado, mesmo que esses clientes estejam usando o mesmo intervalo de sub-rede de endereço IP. Isso permite a separação do tráfego do cliente para privacidade e segurança.

Um espaço IPspace define um espaço de endereço IP distinto no qual as máquinas virtuais de armazenamento (SVMs) residem. As portas e os endereços IP definidos para um espaço IP são aplicáveis apenas nesse espaço IPspace. Uma tabela de roteamento distinta é mantida para cada SVM em um IPspace. Portanto, não ocorre roteamento de tráfego entre SVM ou entre IPspace.

Os IPspaces suportam endereços IPv4 e IPv6 em seus domínios de roteamento.

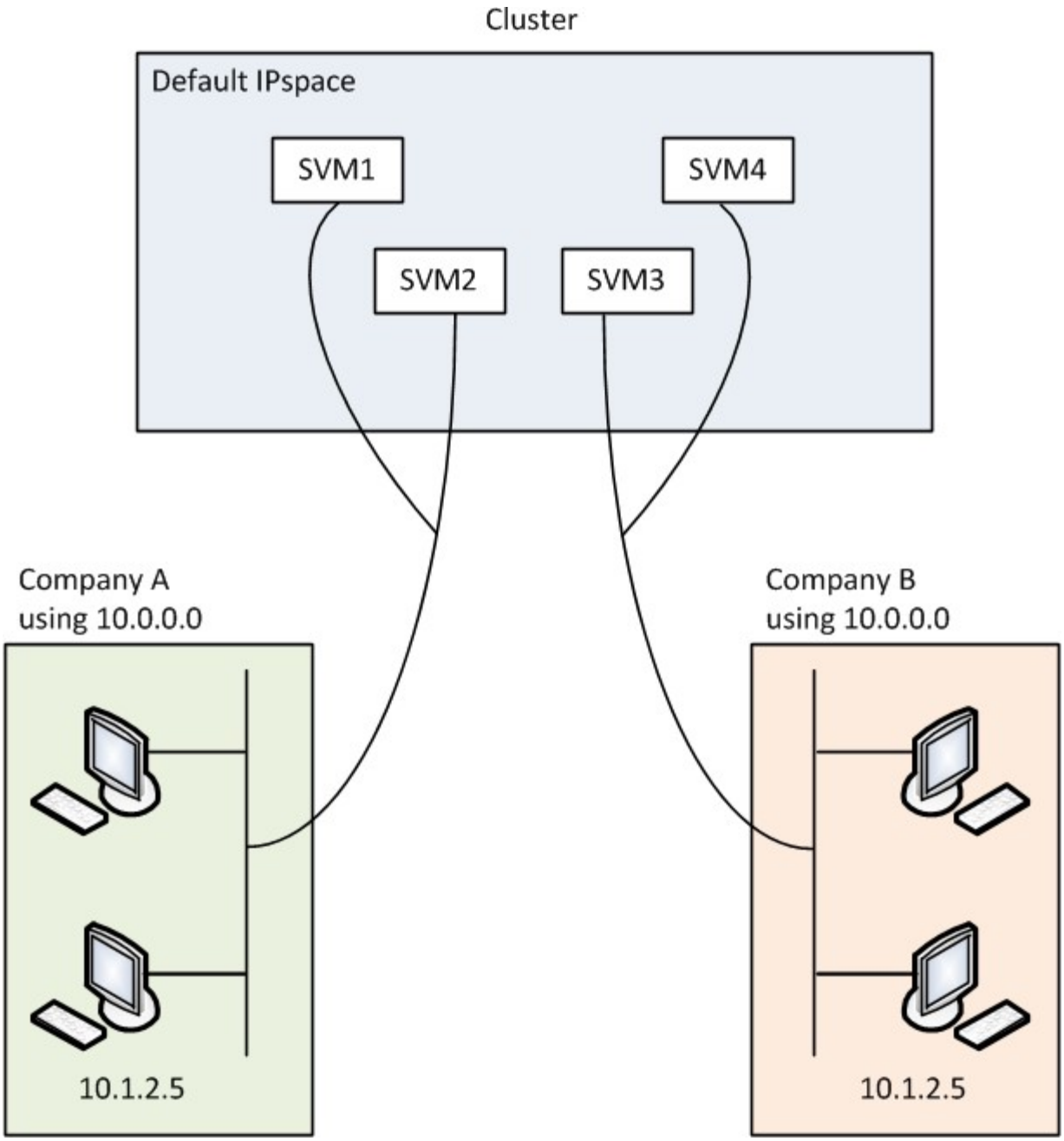
Se você estiver gerenciando o armazenamento para uma única organização, não será necessário configurar os IPspaces. Se você estiver gerenciando o armazenamento para várias empresas em um único cluster do ONTAP e tiver certeza de que nenhum dos seus clientes tem configurações de rede conflitantes, você também não precisa usar espaços IPspaces. Em muitos casos, o uso de máquinas virtuais de armazenamento (SVMs), com suas próprias tabelas de roteamento IP distintas, pode ser usado para segregar configurações de rede exclusivas em vez de usar IPspaces.

Exemplo de uso de IPspaces

Um aplicativo comum para usar espaços IPspaces é quando um provedor de serviços de armazenamento (SSP) precisa conetar clientes das empresas A e B a um cluster ONTAP nas instalações do SSP e ambas as empresas estão usando os mesmos intervalos de endereços IP privados.

O SSP cria SVMs no cluster para cada cliente e fornece um caminho de rede dedicado de dois SVMs para a rede da empresa A e dos outros dois SVMs para a rede da empresa B.

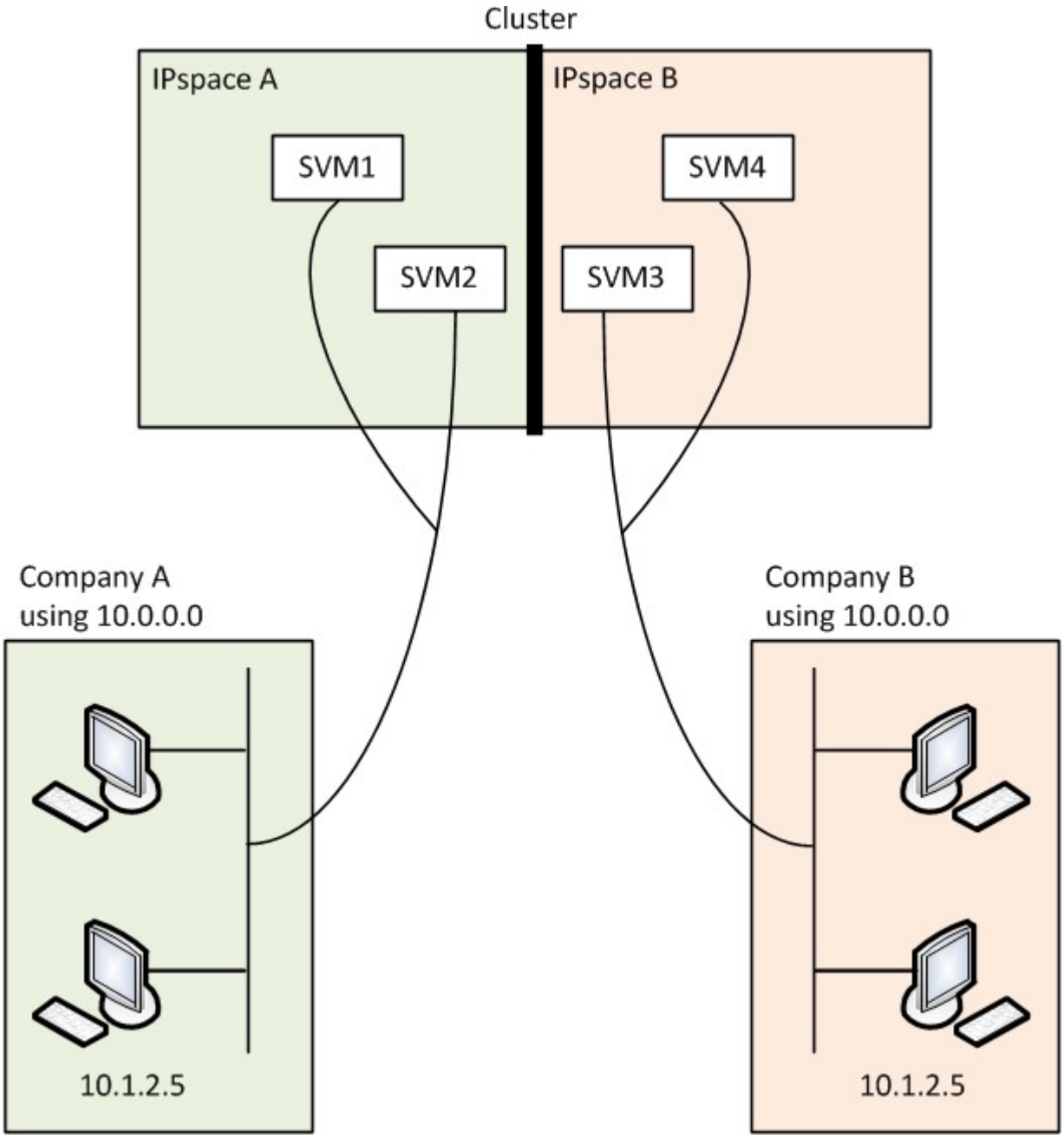
Esse tipo de implantação é mostrado na ilustração a seguir e funciona se ambas as empresas usarem intervalos de endereços IP não privados. No entanto, a ilustração mostra ambas as empresas que usam os mesmos intervalos de endereços IP privados, o que causa problemas.



Ambas as empresas usam a sub-rede de endereço IP privado 10,0.0,0, causando os seguintes problemas:

- Os SVMs no cluster no local SSP têm endereços IP conflitantes se ambas as empresas decidirem usar o mesmo endereço IP para seus respetivos SVMs.
- Mesmo que as duas empresas concordem em usar endereços IP diferentes para seus SVMs, problemas podem surgir.
- Por exemplo, se qualquer cliente na rede De Um tiver o mesmo endereço IP que um cliente na rede B, os pacotes destinados a um cliente no espaço de endereço De Um podem ser roteados para um cliente no espaço de endereço de B e vice-versa.
- Se as duas empresas decidirem usar espaços de endereço mutuamente exclusivos (por exemplo, A usa 10.0.0.0 com uma máscara de rede de 255.128.0.0 e B usa 10.128.0.0 com uma máscara de rede de 255.128.0.0), o SSP precisa configurar rotas estáticas no cluster para rotear o tráfego adequadamente para as redes A e B.

- Essa solução não é escalável (por causa de rotas estáticas) nem segura (o tráfego de broadcast é enviado para todas as interfaces do cluster). Para superar esses problemas, o SSP define dois IPspaces no cluster – um para cada empresa. Como nenhum tráfego cross-IPspace é roteado, os dados de cada empresa são roteados com segurança para sua respetiva rede, mesmo que todos os SVMs estejam configurados no espaço de endereço 10.0.0.0, como mostrado na ilustração a seguir:



Além disso, os endereços IP referidos pelos vários arquivos de configuração, como o `/etc/ hosts` arquivo, o `/etc/hosts.equiv` arquivo e `the /etc/rc` o arquivo, são relativos a esse espaço IPspace. Portanto, os IPspaces permitem que o SSP configure o mesmo endereço IP para os dados de configuração e autenticação para vários SVMs, sem conflito.

Propriedades padrão de IPspaces

IPspaces especiais são criados por padrão quando o cluster é criado pela primeira vez. Além disso, máquinas virtuais de armazenamento especiais (SVMs) são criadas para cada espaço IPspace.

Dois IPspaces são criados automaticamente quando o cluster é inicializado:

- Espaço IPspace "predefinido"

  Esse IPspace é um contêiner para portas, sub-redes e SVMs que atendem dados. Se sua configuração não precisar de IPspaces separados para clientes, todos os SVMs podem ser criados neste IPspace. Este IPspace também contém o gerenciamento de cluster e as portas de gerenciamento de nós.

- Espaço IPspace "cluster"

  Este espaço IPspace contém todas as portas de cluster de todos os nós do cluster. Ele é criado automaticamente quando o cluster é criado. Ele fornece conetividade à rede interna de cluster privado. À medida que nós adicionais se juntam ao cluster, as portas de cluster desses nós são adicionadas ao espaço IPspace "Cluster".

Existe um SVM de "sistema" para cada espaço de IPspace. Quando você cria um IPspace, um SVM do sistema padrão com o mesmo nome é criado:

- O sistema SVM para o IPspace "Cluster" transporta o tráfego de cluster entre nós de um cluster na rede interna de cluster privado.

  Ele é gerenciado pelo administrador do cluster e tem o nome "Cluster".

- O SVM do sistema para o IPspace "padrão" transporta o tráfego de gerenciamento para o cluster e nós, incluindo o tráfego entre clusters.

  Ele é gerenciado pelo administrador do cluster e usa o mesmo nome do cluster.

- O SVM do sistema de um IPspace personalizado que você cria transporta o tráfego de gerenciamento para esse SVM.

  Ele é gerenciado pelo administrador do cluster e usa o mesmo nome que o IPspace.

Um ou mais SVMs para clientes podem existir em um IPspace. Cada SVM de cliente tem seus próprios volumes e configurações de dados, e é administrado independentemente de outras SVMs.

Crie IPspaces

Os IPspaces são espaços de endereço IP distintos nos quais as máquinas virtuais de armazenamento (SVMs) residem. Você pode criar IPspaces quando precisar que seus SVMs tenham seu próprio armazenamento, administração e roteamento seguros. Você pode usar um espaço de IPspace para criar um espaço de endereço IP distinto para cada SVM em um cluster. Isso permite que os clientes em domínios de rede separados administrativamente acessem os dados do cluster ao usar endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Sobre esta tarefa

Há um limite de 512 IPspaces em todo o cluster. O limite de todo o cluster é reduzido para 256 IPspaces para clusters que contêm nós com 6 GB de RAM. Consulte o Hardware Universe para determinar se limites adicionais se aplicam à sua plataforma.

"NetApp Hardware Universe"

Um nome IPspace não pode ser "All" porque "All" é um nome reservado ao sistema.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Criar um espaço IPspace:

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` É o nome do IPspace que você deseja criar. O comando a seguir cria o IPspace ipspace1 em um cluster:

```
network ipspace create -ipspace ipspace1
```

2. Apresentar os IPspaces:

`network ipspace show`

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

O IPspace é criado, juntamente com o sistema SVM para o IPspace. O SVM do sistema transporta tráfego de gerenciamento.

Depois de terminar

Se você criar um espaço de IPspace em um cluster com uma configuração MetroCluster, os objetos de IPspace devem ser replicados manualmente para os clusters de parceiros. Quaisquer SVMs criadas e atribuídas a um IPspace antes da replicação do IPspace não serão replicadas para os clusters de parceiros.

Os domínios de broadcast são criados automaticamente no IPspace "padrão" e podem ser movidos entre IPspaces usando o seguinte comando:

```
network port broadcast-domain move
```

Por exemplo, se você quiser mover um domínio de broadcast de "padrão" para "IPS1", usando o seguinte comando:

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

Apresentar IPspaces

Você pode exibir a lista de IPspaces que existem em um cluster e pode exibir as máquinas virtuais de armazenamento (SVMs), domínios de broadcast e portas que são atribuídas a cada IPspace.

Passo

Exibir os IPspaces e SVMs em um cluster:

```
network ipspace show [-ipspace ipspace_name]
```

O comando a seguir exibe todos os domínios IPspaces, SVMs e broadcast no cluster:

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

O comando a seguir exibe os nós e as portas que fazem parte do IPspace ipspace1:

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

Exclua um espaço IPspace

Se você não precisar mais de um IPspace, você pode excluí-lo.

Antes de começar

Não deve haver domínios de broadcast, interfaces de rede ou SVMs associados ao IPspace que você deseja excluir.

Os espaços IPspaces "Default" e "Cluster" definidos pelo sistema não podem ser eliminados.

Passo

Eliminar um espaço IPspace:

```
network ipspace delete -ipspace ipspace_name
```

O comando a seguir exclui o IPspace ipspace1 do cluster:

```
network ipspace delete -ipspace ipspace1
```

Domínios de broadcast

Domínio de transmissão (ONTAP 9 .8 e posterior)

Visão geral do domínio de broadcast (ONTAP 9.8 e posterior)

Os domínios de broadcast destinam-se a agrupar portas de rede que pertencem à mesma rede de camada 2. As portas do grupo podem ser usadas por uma máquina virtual de storage (SVM) para tráfego de dados ou gerenciamento.

Um domínio de broadcast reside em um IPspace. Durante a inicialização do cluster, o sistema cria dois domínios de broadcast padrão:

- O domínio de broadcast "padrão" contém portas que estão no espaço IPspace "padrão".

  Essas portas são usadas principalmente para fornecer dados. As portas de gerenciamento de clusters e de nós também estão neste domínio de transmissão.

- O domínio de broadcast "Cluster" contém portas que estão no espaço IPspace "Cluster".

  Essas portas são usadas para comunicação de cluster e incluem todas as portas de cluster de todos os nós no cluster.

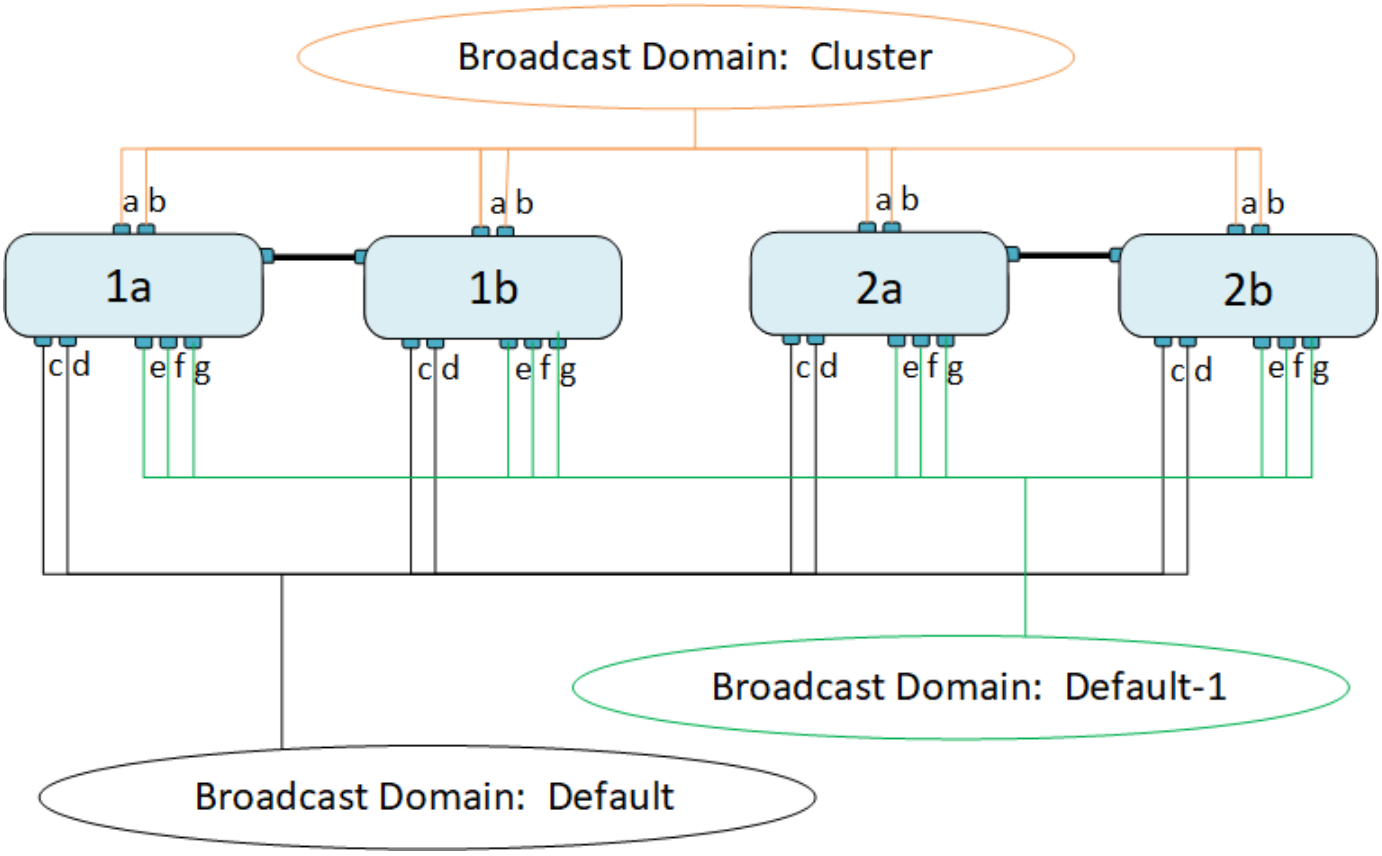
  O sistema cria domínios de broadcast adicionais no IPspace padrão quando necessário. O domínio de broadcast "padrão" contém a porta inicial do LIF de gerenciamento, além de quaisquer outras portas que tenham acessibilidade da camada 2 a essa porta. Domínios de broadcast adicionais são denominados "default-1", "default-2", e assim por diante.

Exemplo de uso de domínios de broadcast

Um domínio de broadcast é um conjunto de portas de rede no mesmo IPspace que também tem acessibilidade da camada 2 umas às outras, normalmente incluindo portas de muitos nós no cluster.

A ilustração mostra as portas atribuídas a três domínios de broadcast em um cluster de quatro nós:

- O domínio de broadcast "Cluster" é criado automaticamente durante a inicialização do cluster e contém as portas a e b de cada nó no cluster.
- O domínio de broadcast "padrão" também é criado automaticamente durante a inicialização do cluster e contém as portas c e d de cada nó no cluster.
- O sistema cria automaticamente quaisquer domínios de broadcast adicionais durante a inicialização do cluster com base na acessibilidade da rede da camada 2. Esses domínios de broadcast adicionais são nomeados default-1, default-2 e assim por diante.



Um grupo de failover com o mesmo nome e com as mesmas portas de rede que cada um dos domínios de broadcast é criado automaticamente. Esse grupo de failover é gerenciado automaticamente pelo sistema, o que significa que, à medida que as portas são adicionadas ou removidas do domínio de broadcast, elas são adicionadas ou removidas automaticamente desse grupo de failover.

Adicione um domínio de broadcast

Os domínios de broadcast agrupam portas de rede no cluster que pertencem à mesma rede de camada 2. As portas podem então ser usadas por SVMs.

A partir do ONTAP 9.8, os domínios de broadcast são criados automaticamente durante a operação de criação ou associação de cluster. A partir do ONTAP 9.12,0, além dos domínios de broadcast criados automaticamente, você pode adicionar manualmente um domínio de broadcast no Gerenciador de sistema.

Antes de começar

As portas que pretende adicionar ao domínio de difusão não devem pertencer a outro domínio de difusão. Se as portas que você deseja usar pertencerem a outro domínio de broadcast, mas não forem utilizadas, remova essas portas do domínio de broadcast original.

Sobre esta tarefa

- Todos os nomes de domínio de broadcast devem ser exclusivos dentro de um espaço IPspace.
- As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de agregação de links/grupos de interface (LAGs/ifgrps).
- Se as portas que você deseja usar pertencerem a outro domínio de broadcast, mas não forem utilizadas, remova-as do domínio de broadcast existente antes de adicioná-las ao novo.
- A unidade máxima de transmissão (MTU) das portas adicionadas a um domínio de broadcast são

atualizadas para o valor MTU definido no domínio de broadcast.

- O valor MTU deve corresponder a todos os dispositivos conetados a essa rede de camada 2, exceto para o tráfego de gerenciamento de manipulação de portas e0M.
- Se você não especificar um nome de IPspace, o domínio de broadcast será criado no IPspace "padrão".

Para facilitar a configuração do sistema, um grupo de failover com o mesmo nome é criado automaticamente que contém as mesmas portas.

System Manager

Passos

1. Selecione **rede > Visão geral > domínio Broadcast**.
2. Clique em + Add
3. Nomeie o domínio de broadcast.
4. Defina a MTU.
5. Selecione o espaço IPspace.
6. Salve o domínio de broadcast.

Você pode editar ou excluir um domínio de broadcast depois que ele foi adicionado.

CLI

No ONTAP 9.7 ou anterior, você pode criar manualmente um domínio de broadcast.

Se você estiver usando o ONTAP 9.8 e posterior, os domínios de broadcast serão criados automaticamente com base na acessibilidade da camada 2. Para obter mais informações, "Acessibilidade da porta de reparo"consulte .

Passos

1. Exibir as portas que não estão atualmente atribuídas a um domínio de broadcast:

   ```
   network port show
   ```

   Se a exibição for grande, use o `network port show -broadcast-domain` comando para exibir somente portas não atribuídas.

2. Criar um domínio de broadcast:

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` é o nome do domínio de broadcast que você deseja criar.

   b. `mtu_value` É o tamanho MTU para pacotes IP; 1500 e 9000 são valores típicos.

      Esse valor é aplicado a todas as portas que são adicionadas a esse domínio de broadcast.

   c. `ipspace_name` É o nome do IPspace ao qual este domínio de broadcast será adicionado.

      O espaço IPspace "padrão" é usado a menos que você especifique um valor para este parâmetro.

   d. `ports_list` é a lista de portas que serão adicionadas ao domínio de broadcast.

      As portas são adicionadas no formato `node_name:port_number`, por exemplo, `node1:e0c`.

3. Verifique se o domínio de broadcast foi criado conforme desejado:

   ```
   network port show -instance -broadcast-domain new_domain
   ```

Exemplo

O comando a seguir cria o domínio de broadcast bcast1 no IPspace padrão, define o MTU como 1500 e adiciona quatro portas:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

Depois de terminar

Você pode definir o pool de endereços IP que estará disponível no domínio de broadcast criando uma sub-rede ou pode atribuir SVMs e interfaces ao IPspace neste momento. Para obter mais informações, "Peering de cluster e SVM"consulte .

Se você precisar alterar o nome de um domínio de broadcast existente, use o `network port broadcast-domain rename` comando.

Adicionar ou remover portas de um domínio de broadcast (ONTAP 9.8 e posterior)

Os domínios de broadcast são criados automaticamente durante a operação de criação ou associação de cluster. Não é necessário remover manualmente as portas dos domínios de broadcast.

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e uma porta de rede pertencer a um domínio de broadcast diferente, consulte o seguinte tópico:

"Acessibilidade da porta de reparo"

System Manager

A partir do ONTAP 9.14,1, você pode usar o Gerenciador do sistema para reatribuir portas Ethernet em domínios de broadcast. É recomendável atribuir todas as portas Ethernet a um domínio de broadcast. Portanto, se você cancelar a atribuição de uma porta Ethernet de um domínio de broadcast, será necessário reatribuí-la a um domínio de broadcast diferente.

Passos

Para reatribuir portas Ethernet, execute as seguintes etapas:

1. Selecione **rede > Visão geral**.
2. Na seção **Broadcast Domains**, selecione ⋮ ao lado do nome de domínio.
3. No menu suspenso, selecione **Editar**.
4. Na página **Editar domínio de transmissão**, desmarque as portas Ethernet que deseja reatribuir a outro domínio.
5. Para cada porta desmarcada, a janela **Reatribuir porta Ethernet** é exibida. Selecione o domínio de broadcast ao qual deseja reatribuir a porta e selecione **Reatribuir**.
6. Selecione todas as portas que você deseja atribuir ao domínio de broadcast atual e salve as alterações.

CLI

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e uma porta de rede pertencer a um domínio de broadcast diferente, consulte o seguinte tópico:

"Acessibilidade da porta de reparo"

Como alternativa, você pode adicionar ou remover portas manualmente de domínios de broadcast usando o `network port broadcast-domain add-ports` comando ou `network port broadcast-domain remove-ports` .

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- As portas que pretende adicionar a um domínio de difusão não devem pertencer a outro domínio de difusão.
- As portas que já pertencem a um grupo de interfaces não podem ser adicionadas individualmente a um domínio de broadcast.

Sobre esta tarefa

As regras a seguir se aplicam ao adicionar e remover portas de rede:

Ao adicionar portas…	Ao remover portas…
As portas podem ser portas de rede, VLANs ou grupos de interface (ifgrps).	N/A.
As portas são adicionadas ao grupo de failover definido pelo sistema do domínio de broadcast.	As portas são removidas de todos os grupos de failover no domínio de broadcast.
A MTU das portas é atualizada para o valor MTU definido no domínio de broadcast.	A MTU das portas não muda.

O IPspace das portas é atualizado para o valor IPspace do domínio de broadcast.	As portas são movidas para o espaço IPspace 'padrão' sem atributo de domínio de broadcast.

Se você remover a última porta membro de um grupo de interfaces usando o `network port ifgrp remove-port` comando, isso fará com que a porta do grupo de interfaces seja removida do domínio de broadcast porque uma porta de grupo de interfaces vazia não é permitida em um domínio de broadcast.

Passos

1. Exiba as portas que estão atualmente atribuídas ou não atribuídas a um domínio de broadcast usando o `network port show` comando.
2. Adicionar ou remover portas de rede do domínio de broadcast:

Se você quiser…	Utilizar…
Adicionar portas a um domínio de broadcast	`network port broadcast-domain add-ports`
Remover portas de um domínio de broadcast	`network port broadcast-domain remove-ports`

3. Verifique se as portas foram adicionadas ou removidas do domínio de broadcast:

   `network port show`

Para obter mais informações sobre esses comandos, consulte "Referência do comando ONTAP"

Exemplos de adição e remoção de portas

O comando a seguir adiciona a porta e0g no cluster de nó-1-01 e a porta e0g no cluster de nó-1-02 para transmitir o domínio bcast1 no IPspace padrão:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

O comando a seguir adiciona duas portas de cluster ao cluster de domínio de broadcast no Cluster IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

O comando a seguir remove a porta e0e no nó cluster1-01 do domínio de broadcast bcast1 no IPspace padrão:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

Acessibilidade da porta de reparo

Domínios de broadcast são criados automaticamente. No entanto, se uma porta for

recarregada ou a configuração do switch mudar, uma porta pode precisar ser reparada em um domínio de broadcast diferente (novo ou existente).

O ONTAP pode detetar e recomendar automaticamente soluções para problemas de fiação de rede com base na acessibilidade da camada 2 de um componente de domínio de transmissão (portas ethernet).

A fiação incorreta durante pode causar uma atribuição inesperada da porta do domínio de broadcast. A partir do ONTAP 9.10,1, o cluster verifica automaticamente problemas de fiação de rede verificando a acessibilidade da porta após a configuração do cluster ou quando um novo nó se junta a um cluster existente.

System Manager

Se for detetado um problema de acessibilidade da porta, o System Manager recomenda uma operação de reparo para resolver o problema.

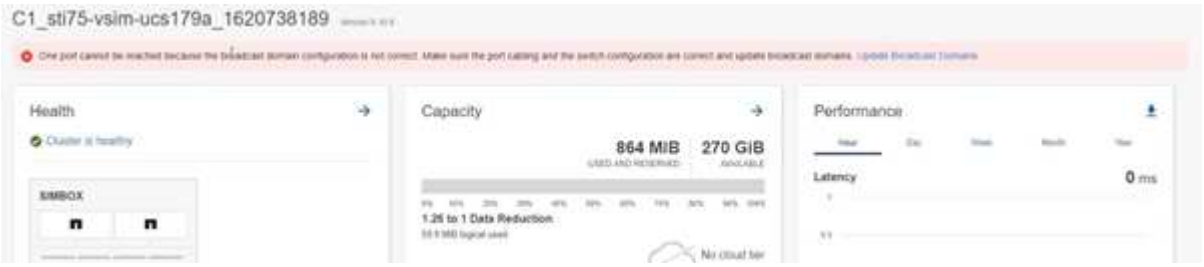
Depois de configurar o cluster, os problemas de fiação de rede são relatados no Dashboard.

Depois de unir um novo nó a um cluster, os problemas de fiação de rede aparecem na página nós.

Também pode ver o estado da cablagem da rede no diagrama da rede. Os problemas de acessibilidade da porta são indicados no diagrama de rede por um ícone de erro vermelho.

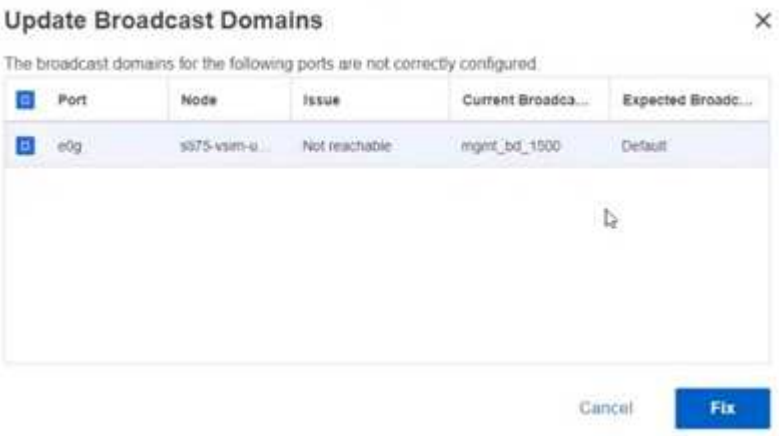
Configuração pós-cluster

Depois de configurar o cluster, se o sistema detetar um problema de fiação de rede, uma mensagem será exibida no Dashboard.



Passos

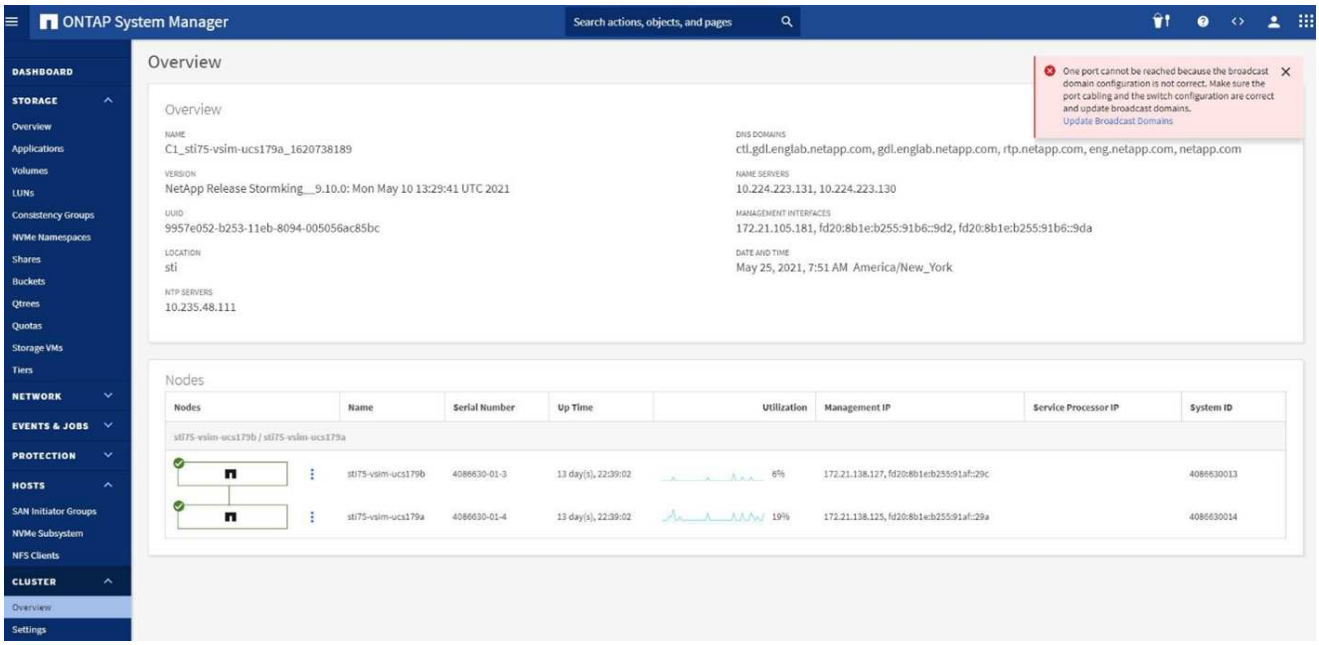
1. Corrija a fiação conforme sugerido na mensagem.
2. Clique no link para iniciar a caixa de diálogo Atualizar domínios de transmissão. A caixa de diálogo Atualizar domínios de transmissão é aberta.



3. Revise as informações sobre a porta, incluindo o nó, os problemas, o domínio de broadcast atual e o domínio de broadcast esperado.
4. Selecione as portas que deseja reparar e clique em **Fix**. O sistema moverá as portas do domínio de broadcast atual para o domínio de broadcast esperado.

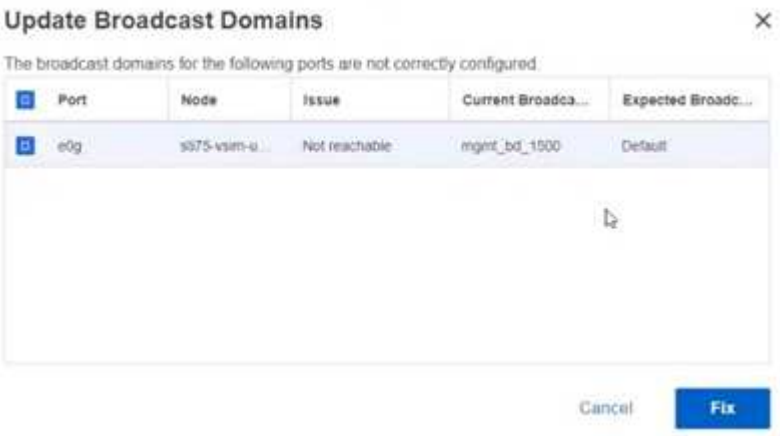
Post node join

Depois de unir um novo nó a um cluster, se o sistema detetar um problema de fiação de rede, uma mensagem será exibida na página nós.



Passos

1. Corrija a fiação conforme sugerido na mensagem.
2. Clique no link para iniciar a caixa de diálogo Atualizar domínios de transmissão. A caixa de diálogo Atualizar domínios de transmissão é aberta.



3. Revise as informações sobre a porta, incluindo o nó, os problemas, o domínio de broadcast atual e o domínio de broadcast esperado.
4. Selecione as portas que deseja reparar e clique em **Fix**. O sistema moverá as portas do domínio de broadcast atual para o domínio de broadcast esperado.

CLI

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Sobre esta tarefa

Um comando está disponível para reparar automaticamente a configuração do domínio de broadcast para uma porta baseada na acessibilidade da camada 2 detetada pelo ONTAP.

Passos

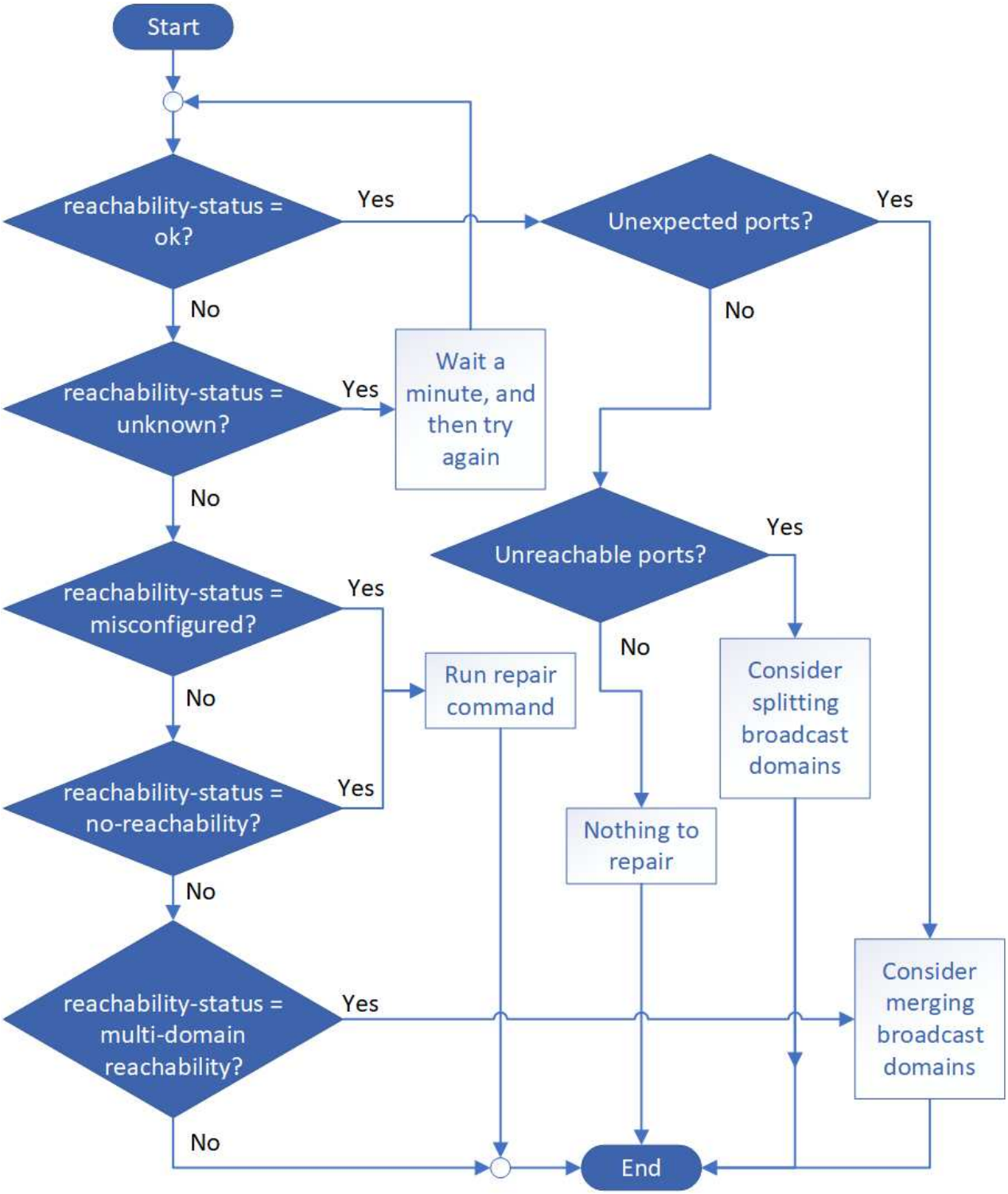
1. Verifique a configuração e o cabeamento do switch.

2. Verifique a acessibilidade da porta:

   ```
   network port reachability show -detail -node -port
   ```

   O comando output contém resultados de acessibilidade.

3. Use a tabela e a árvore de decisão a seguir para entender os resultados de acessibilidade e determinar o que, se alguma coisa, fazer a seguir.



Status de acessibilidade	Descrição
ok	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído. Se o status de acessibilidade for "ok", mas houver "portas inesperadas", considere mesclar um ou mais domínios de broadcast. Para obter mais informações, consulte a seguinte linha *portas inesperadas*. Se o status de acessibilidade for "ok", mas houver "portas inalcançáveis", considere dividir um ou mais domínios de broadcast. Para obter mais informações, consulte a seguinte linha *portas inalcançáveis*. Se o status de acessibilidade for "ok" e não houver portas inesperadas ou inacessíveis, sua configuração está correta.
Portas inesperadas	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast. Examine a conetividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast. Para obter mais informações, "Mesclar domínios de broadcast"consulte .
Portas inalcançáveis	Se um único domínio de broadcast tiver sido particionado em dois conjuntos de acessibilidade diferentes, você poderá dividir um domínio de broadcast para sincronizar a configuração do ONTAP com a topologia de rede física. Normalmente, a lista de portas inalcançáveis define o conjunto de portas que devem ser divididas em outro domínio de broadcast depois de ter verificado que a configuração física e do switch é precisa. Para obter mais informações, "Dividir domínios de broadcast"consulte .
acessibilidade mal configurada	A porta não tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, a porta tem acessibilidade da camada 2 para um domínio de broadcast diferente. Você pode reparar a acessibilidade da porta. Ao executar o seguinte comando, o sistema atribuirá a porta ao domínio de broadcast ao qual tem acessibilidade: `network port reachability repair -node -port`

sem acessibilidade	A porta não tem acessibilidade da camada 2 para qualquer domínio de broadcast existente. Você pode reparar a acessibilidade da porta. Quando você executa o seguinte comando, o sistema atribuirá a porta a um novo domínio de broadcast criado automaticamente no IPspace padrão: `network port reachability repair -node -port` **Nota:** se todas as portas membros do grupo de interfaces (ifgrp) reportarem `no-reachability`, executar o `network port reachability repair` comando em cada porta membro faria com que cada uma fosse removida do ifgrp e colocada em um novo domínio de broadcast, eventualmente fazendo com que o próprio ifgrp fosse removido. Antes de executar o `network port reachability repair` comando, verifique se o domínio de broadcast acessível da porta é o que você espera com base na topologia física da rede.
multidomínio-acessibilidade	A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast. Examine a conetividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast. Para obter mais informações, "Mesclar domínios de broadcast"consulte .
desconhecido	Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.

Depois de reparar uma porta, verifique se há LIFs e VLANs deslocados. Se a porta fazia parte de um grupo de interfaces, você também precisa entender o que aconteceu com esse grupo de interfaces.

LIFs

Quando uma porta é reparada e movida para um domínio de broadcast diferente, todos os LIFs que foram configurados na porta reparada receberão automaticamente uma nova porta inicial. Essa porta inicial é selecionada a partir do mesmo domínio de broadcast no mesmo nó, se possível. Alternativamente, uma porta inicial de outro nó é selecionada ou, se não existirem portas residenciais adequadas, a porta inicial será limpa.

Se a porta inicial de um LIF for movida para outro nó ou for limpa, então o LIF é considerado como "deslocado". Você pode visualizar esses LIFs deslocados com o seguinte comando:

```
displaced-interface show
```

Se houver LIFs deslocados, você deve:

- Restaure a casa do LIF deslocado:

  ```
  displaced-interface restore
  ```

- Defina a casa do LIF manualmente:

```
network interface modify -home-port -home-node
```

- Remova a entrada da tabela "interface deslocada" se estiver satisfeito com a página inicial atualmente configurada do LIF:

```
displaced-interface delete
```

VLANs

Se a porta reparada tivesse VLANs, essas VLANs serão excluídas automaticamente, mas também serão registradas como tendo sido "deslocadas". Você pode exibir essas VLANs deslocadas:

```
displaced-vlans show
```

Se houver quaisquer VLANs deslocadas, você deve:

- Restaure as VLANs para outra porta:

```
displaced-vlans restore
```

- Remova a entrada da tabela "Displaced-vlans":

```
displaced-vlans delete
```

Grupos de interfaces

Se a porta reparada fizer parte de um grupo de interfaces, ela será removida desse grupo de interfaces. Se fosse a única porta membro atribuída ao grupo de interfaces, o próprio grupo de interfaces será removido.

Tópicos relacionados

"Verifique a configuração da rede após a atualização"

"Monitore a acessibilidade das portas de rede"

Mover domínios de broadcast para IPspaces (ONTAP 9.8 e posterior)

Mova os domínios de broadcast criados pelo sistema com base na acessibilidade da camada 2 para os IPspaces criados.

Antes de mover o domínio de broadcast, você deve verificar a acessibilidade das portas em seus domínios de broadcast.

A verificação automática das portas pode determinar quais portas podem alcançar umas às outras e colocá-las no mesmo domínio de broadcast, mas essa verificação não consegue determinar o espaço IPspace apropriado. Se o domínio de broadcast pertencer a um espaço IPspace não padrão, você deve movê-lo manualmente usando as etapas desta seção.

Antes de começar

Os domínios de broadcast são configurados automaticamente como parte das operações de criação e associação de cluster. O ONTAP define o domínio de broadcast "padrão" como o conjunto de portas que têm conetividade de camada 2 à porta inicial da interface de gerenciamento no primeiro nó criado no cluster. Outros domínios de broadcast são criados, se necessário, e são nomeados **default-1**, **default-2**, e assim por

diante.

Quando um nó se une a um cluster existente, suas portas de rede se juntam automaticamente aos domínios de broadcast existentes com base em sua acessibilidade da camada 2. Se eles não tiverem acessibilidade a um domínio de broadcast existente, as portas serão colocadas em um ou mais novos domínios de broadcast.

Sobre esta tarefa

- As portas com LIFs de cluster são colocadas automaticamente no espaço IPspace "Cluster".
- As portas com acessibilidade à porta inicial do LIF de gerenciamento de nó são colocadas no domínio de broadcast "padrão".
- Outros domínios de broadcast são criados automaticamente pelo ONTAP como parte da operação de criação ou associação de cluster.
- À medida que você adiciona VLANs e grupos de interface, eles são automaticamente colocados no domínio de broadcast apropriado cerca de um minuto após serem criados.

Passos

1. Verifique a acessibilidade das portas em seus domínios de broadcast. O ONTAP monitora automaticamente a acessibilidade da camada 2. Use o seguinte comando para verificar se cada porta foi adicionada a um domínio de broadcast e tem acessibilidade "ok".

   ```
   network port reachability show -detail
   ```

2. Se necessário, mova domínios de broadcast para outros IPspaces:

   ```
   network port broadcast-domain move
   ```

   Por exemplo, se você quiser mover um domínio de broadcast de "padrão" para "IPS1":

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

Domínios de broadcast divididos (ONTAP 9.8 e posteriores)

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e um grupo de portas de rede previamente configuradas em um único domínio de broadcast tiver sido particionado em dois conjuntos de acessibilidade diferentes, você pode dividir um domínio de broadcast para sincronizar a configuração do ONTAP com a topologia de rede física.

Para determinar se um domínio de broadcast de porta de rede está particionado em mais de um conjunto de acessibilidade, use o `network port reachability show -details` comando e preste atenção às portas que não têm conetividade entre si ("portas inacessíveis"). Normalmente, a lista de portas inalcançáveis define o conjunto de portas que devem ser divididas em outro domínio de broadcast, depois de ter verificado que a configuração física e do switch é precisa.

Passo

Divida um domínio de broadcast em dois domínios de broadcast:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` é o nome do ipspace onde reside o domínio de broadcast.
- `-broadcast-domain` é o nome do domínio de broadcast que será dividido.
- `-new-broadcast-domain` é o nome do novo domínio de broadcast que será criado.
- `-ports` é o nome e a porta do nó a serem adicionados ao novo domínio de broadcast.

Mesclar domínios de broadcast (ONTAP 9.8 e posterior)

Se a acessibilidade da porta de rede tiver sido alterada, seja por meio de conetividade de rede física ou configuração de switch, e dois grupos de portas de rede previamente configurados em vários domínios de broadcast agora todos compartilham acessibilidade, a mesclagem de dois domínios de broadcast pode ser usada para sincronizar a configuração do ONTAP com a topologia de rede física.

Para determinar se vários domínios de broadcast pertencem a um conjunto de acessibilidade, use o comando "network port alcançability show -details" e preste atenção às portas que são configuradas em outro domínio de broadcast realmente têm conetividade entre si ("portas inesperadas"). Normalmente, a lista de portas inesperadas define o conjunto de portas que devem ser mescladas no domínio de broadcast depois de verificar se a configuração física e do switch é precisa.

Passo

Mesclar as portas de um domínio de broadcast em um domínio de broadcast existente:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` é o nome do ipspace onde os domínios de broadcast residem.
- `-broadcast-domain` é o nome do domínio de broadcast que será mesclado.
- `-into-broadcast-domain` é o nome do domínio de broadcast que receberá portas adicionais.

Alterar o valor MTU para portas em um domínio de broadcast (ONTAP 9.8 e posterior)

Você pode modificar o valor MTU de um domínio de broadcast para alterar o valor MTU para todas as portas nesse domínio de broadcast. Isso pode ser feito para suportar alterações de topologia que foram feitas na rede.

Antes de começar

O valor MTU deve corresponder a todos os dispositivos conetados a essa rede de camada 2, exceto para o tráfego de gerenciamento de manipulação de portas e0M.

Sobre esta tarefa

A alteração do valor MTU provoca uma breve interrupção no tráfego nas portas afetadas. O sistema exibe um prompt que você deve responder com y para fazer a alteração da MTU.

Passo

Altere o valor MTU para todas as portas em um domínio de broadcast:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` é o nome do domínio de broadcast.
- `mtu` É o tamanho MTU para pacotes IP; 1500 e 9000 são valores típicos.
- `ipspace` É o nome do IPspace no qual esse domínio de broadcast reside. O espaço IPspace "padrão" é usado a menos que você especifique um valor para esta opção. O comando a seguir altera o MTU para 9000 para todas as portas no domínio de broadcast bcast1:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

Exibir domínios de broadcast (ONTAP 9.8 e posteriores)

Você pode exibir a lista de domínios de broadcast dentro de cada espaço IPspace em um cluster. A saída também mostra a lista de portas e o valor MTU para cada domínio de broadcast.

Passo

Exiba os domínios de broadcast e as portas associadas no cluster:

```
network port broadcast-domain show
```

O comando a seguir exibe todos os domínios de broadcast e portas associadas no cluster:

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

O comando a seguir exibe as portas no domínio de broadcast padrão-1 que têm um status de atualização de erro, o que indica que a porta não pôde ser atualizada corretamente:

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Default Default-1    1500
                           cluster-1-02:e0g       error
```

Para obter mais informações, consulte "Referência do comando ONTAP" .

Excluir um domínio de broadcast

Se você não precisar mais de um domínio de broadcast, você pode excluí-lo. Isso move as portas associadas a esse domínio de broadcast para o espaço IPspace "padrão".

Antes de começar

Não deve haver sub-redes, interfaces de rede ou SVMs associadas ao domínio de broadcast que você deseja excluir.

Sobre esta tarefa

- O domínio de broadcast "Cluster" criado pelo sistema não pode ser excluído.
- Todos os grupos de failover relacionados ao domínio de broadcast são removidos quando você exclui o domínio de broadcast.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador de sistema para excluir um domínio de broadcast

A opção de exclusão não é exibida quando o domínio de broadcast contém portas ou está associado a uma sub-rede.

Passos

1. Selecione **rede > Visão geral > domínio Broadcast**.
2. Selecione **> Excluir** ao lado do domínio de broadcast que deseja remover.

CLI

Use a CLI para excluir um domínio de broadcast

Passo

Excluir um domínio de broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

O seguinte comando exclui o domínio de broadcast default-1 no IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Domínio de broadcast (ONTAP 9 .7 e anteriores)

Visão geral do domínio de broadcast (ONTAP 9 .7 e anteriores)

Os domínios de broadcast destinam-se a agrupar portas de rede que pertencem à mesma rede de camada 2. As portas do grupo podem ser usadas por uma máquina virtual de storage (SVM) para tráfego de dados ou gerenciamento.

Um domínio de broadcast reside em um IPspace. Durante a inicialização do cluster, o sistema cria dois domínios de broadcast padrão:

- O domínio de broadcast padrão contém portas que estão no IPspace padrão. Essas portas são usadas principalmente para fornecer dados. As portas de gerenciamento de clusters e de nós também estão neste domínio de transmissão.
- O domínio de broadcast de cluster contém portas que estão no espaço de IPspace de cluster. Essas portas são usadas para comunicação de cluster e incluem todas as portas de cluster de todos os nós no cluster.

Se você criou IPspaces exclusivos para separar o tráfego do cliente, então você precisa criar um domínio de broadcast em cada um desses IPspaces.

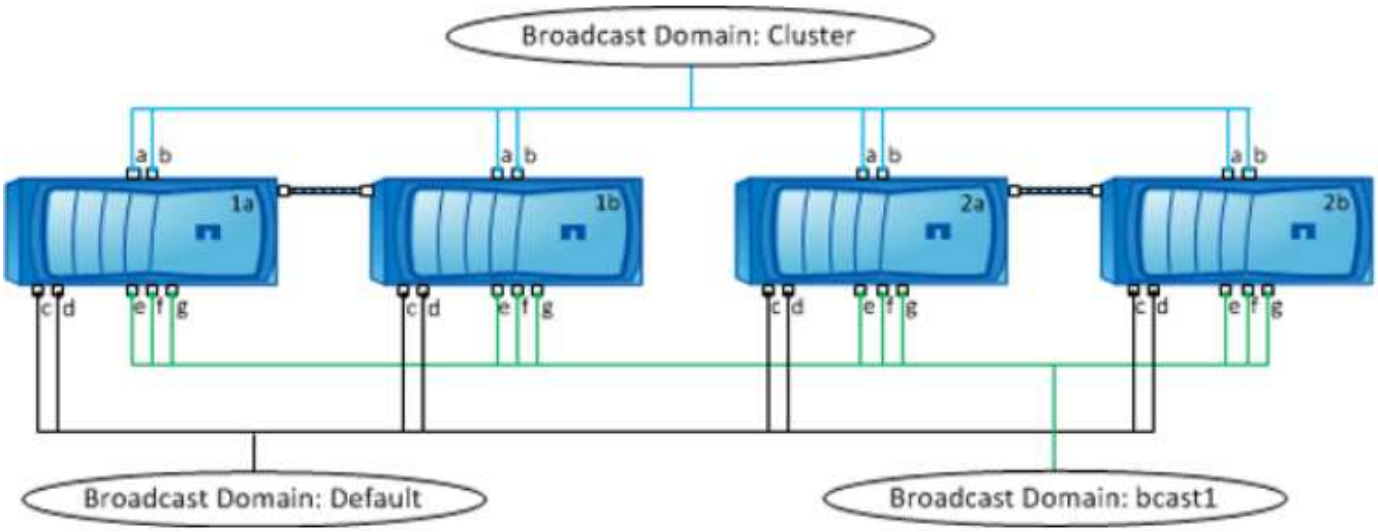
Crie um domínio de broadcast para agrupar portas de rede no cluster que pertencem à mesma rede de camada 2. As portas podem então ser usadas por SVMs.

Exemplo de uso de domínios de broadcast

Um domínio de broadcast é um conjunto de portas de rede no mesmo IPspace que também tem acessibilidade da camada 2 umas às outras, normalmente incluindo portas de muitos nós no cluster.

A ilustração mostra as portas atribuídas a três domínios de broadcast em um cluster de quatro nós:

- O domínio de broadcast de cluster é criado automaticamente durante a inicialização do cluster e contém as portas a e b de cada nó no cluster.
- O domínio de broadcast padrão também é criado automaticamente durante a inicialização do cluster e contém as portas c e d de cada nó no cluster.
- O domínio de broadcast bcast1 foi criado manualmente e contém as portas e, f e g de cada nó no cluster. Esse domínio de broadcast foi criado pelo administrador do sistema especificamente para que um novo cliente acesse dados por meio de um novo SVM.



Um grupo de failover com o mesmo nome e com as mesmas portas de rede que cada um dos domínios de broadcast é criado automaticamente. Esse grupo de failover é gerenciado automaticamente pelo sistema, o que significa que, à medida que as portas são adicionadas ou removidas do domínio de broadcast, elas são adicionadas ou removidas automaticamente desse grupo de failover.

Determinando quais portas podem ser usadas para um domínio de broadcast (ONTAP 9.7 e anteriores)

Antes de configurar um domínio de broadcast para adicionar ao novo espaço IPspace, você deve determinar quais portas estão disponíveis para o domínio de broadcast.

Esta tarefa é relevante para o ONTAP 9.0 - 9,7, não para o ONTAP 9.8.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Sobre esta tarefa

- As portas podem ser portas físicas, VLANs ou grupos de interface (ifgroups).
- As portas que você deseja adicionar ao novo domínio de broadcast não podem ser atribuídas a um domínio de broadcast existente.
- Se as portas que você deseja adicionar ao domínio de broadcast já estiverem em outro domínio de broadcast (por exemplo, o domínio de broadcast padrão no IPspace padrão), remova as portas desse domínio de broadcast antes de atribuí-las ao novo domínio de broadcast.
- As portas que têm LIFs atribuídas a elas não podem ser removidas de um domínio de broadcast.
- Como as LIFs de gerenciamento de cluster e de nó são atribuídas ao domínio de broadcast padrão no IPspace padrão, as portas atribuídas a esses LIFs não podem ser removidas do domínio de broadcast padrão.

Passos

1. Determine as atribuições de portas atuais.

   `network port show`

   ```
   Node   Port IPspace  Broadcast Domain Link   MTU  Admin/Oper
   ------ ---- -------  ---------------- ----- ----  ------------
   node1
          e0a  Cluster  Cluster          up    9000  auto/1000
          e0b  Cluster  Cluster          up    9000  auto/1000
          e0c  Default  Default          up    1500  auto/1000
          e0d  Default  Default          up    1500  auto/1000
          e0e  Default  Default          up    1500  auto/1000
          e0f  Default  Default          up    1500  auto/1000
          e0g  Default  Default          up    1500  auto/1000
   node2
          e0a  Cluster  Cluster          up    9000  auto/1000
          e0b  Cluster  Cluster          up    9000  auto/1000
          e0c  Default  Default          up    1500  auto/1000
          e0d  Default  Default          up    1500  auto/1000
          e0e  Default  Default          up    1500  auto/1000
          e0f  Default  Default          up    1500  auto/1000
          e0g  Default  Default          up    1500  auto/1000
   ```

   Neste exemplo, a saída do comando fornece as seguintes informações:

   - As portas `e0c`, `e0d`, `e0e`, `e0f` e `e0g` em cada nó são atribuídas ao domínio de broadcast padrão.
   - Essas portas estão potencialmente disponíveis para uso no domínio de broadcast do IPspace que você deseja criar.

2. Determine quais portas no domínio de broadcast padrão são atribuídas a interfaces LIF e, portanto, não podem ser movidas para um novo domínio de broadcast.

   `network interface show`

```
         Logical      Status     Network          Current   Current Is
Vserver  Interface    Admin/Oper Address/Mask     Node      Port    Home
-------  ----------   ---------- ------------   --------- -------  ----
Cluster
         node1_clus1  up/up       10.0.2.40/24   node1     e0a     true
         node1_clus2  up/up       10.0.2.41/24   node1     e0b     true
         node2_clus1  up/up       10.0.2.42/24   node2     e0a     true
         node2_clus2  up/up       10.0.2.43/24   node2     e0b     true

cluster1
         cluster_mgmt up/up       10.0.1.41/24   node1     e0c     true
         node1_mgmt   up/up       10.0.1.42/24   node1     e0c     true
         node2_mgmt   up/up       10.0.1.43/24   node2     e0c     true
```

No exemplo a seguir, a saída do comando fornece as seguintes informações:

- As portas do nó são atribuídas à porta `e0c` em cada nó e o nó inicial do LIF administrativo do cluster está `e0c` ligado em `node1`.
- As portas `e0d`, `e0e`, `e0f` e `e0g` em cada nó não hospedam LIFs e podem ser removidas do domínio de broadcast padrão e adicionadas a um novo domínio de broadcast para o novo IPspace.

Criar um domínio de broadcast (ONTAP 9.7 e anteriores)

No ONTAP 9.7 e anteriores, você cria um domínio de broadcast para agrupar portas de rede no cluster que pertencem à mesma rede de camada 2. As portas podem então ser usadas por SVMs. Você deve criar um domínio de broadcast para um IPspace personalizado. As SVMs criadas no IPspace usam as portas no domínio de broadcast.

Esta tarefa é relevante para o ONTAP 9.0 - 9,7, não para o ONTAP 9.8.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

A partir do ONTAP 9.8, os domínios de broadcast são criados automaticamente durante a operação de criação ou associação de cluster. Se você estiver executando o ONTAP 9.8 ou posterior, essas etapas não serão necessárias.

No ONTAP 9.7 e anteriores, as portas que você planeja adicionar ao domínio de broadcast não devem pertencer a outro domínio de broadcast.

Sobre esta tarefa

A porta para a qual um LIF falha deve ser membro do grupo de failover para o LIF. Quando você cria um domínio de broadcast, o ONTAP cria automaticamente um grupo de failover com o mesmo nome. O grupo failover contém todas as portas atribuídas ao domínio de broadcast.

- Todos os nomes de domínio de broadcast devem ser exclusivos dentro de um espaço IPspace.
- As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de interface (ifgrps).

- Se as portas que você deseja usar pertencerem a outro domínio de broadcast, mas não forem utilizadas, use o `network port broadcast-domain remove-ports` comando para remover as portas do domínio de broadcast existente.
- A MTU das portas adicionadas a um domínio de broadcast é atualizada para o valor MTU definido no domínio de broadcast.
- O valor MTU deve corresponder a todos os dispositivos conetados a essa rede de camada 2, exceto para o tráfego de gerenciamento de manipulação de portas e0M.
- Se você não especificar um nome de IPspace, o domínio de broadcast será criado no IPspace "padrão".

Para facilitar a configuração do sistema, um grupo de failover com o mesmo nome é criado automaticamente que contém as mesmas portas.

Passos

1. Exibir as portas que não estão atualmente atribuídas a um domínio de broadcast:

   `network port show`

   Se a exibição for grande, use o `network port show -broadcast-domain` comando para exibir somente portas não atribuídas.

2. Criar um domínio de broadcast:

   `network port broadcast-domain create -broadcast-domain broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]`

   - *`broadcast_domain_name`* é o nome do domínio de broadcast que você deseja criar.
   - *`mtu_value`* É o tamanho MTU para pacotes IP; 1500 e 9000 são valores típicos.

     Esse valor é aplicado a todas as portas que são adicionadas a esse domínio de broadcast.

   - *`ipspace_name`* É o nome do IPspace ao qual este domínio de broadcast será adicionado.

     O espaço IPspace "padrão" é usado a menos que você especifique um valor para este parâmetro.

   - *`ports_list`* é a lista de portas que serão adicionadas ao domínio de broadcast.

     As portas são adicionadas no formato *`node_name:port_number`*, por exemplo, `node1:e0c`.

3. Verifique se o domínio de broadcast foi criado conforme desejado:
   `network port show -instance -broadcast-domain new_domain`

Exemplo

O comando a seguir cria o domínio de broadcast bcast1 no IPspace padrão, define o MTU como 1500 e adiciona quatro portas:

`network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f`

Depois de terminar

Você pode definir o pool de endereços IP que estará disponível no domínio de broadcast criando uma sub-rede ou pode atribuir SVMs e interfaces ao IPspace neste momento. Para obter mais informações, "Peering

de cluster e SVM"consulte .

Se você precisar alterar o nome de um domínio de broadcast existente, use o `network port broadcast-domain rename` comando.

Adicionar ou remover portas de um domínio de broadcast (ONTAP 9.7 e anterior)

Você pode adicionar portas de rede ao criar inicialmente um domínio de broadcast ou adicionar portas ou remover portas de um domínio de broadcast que já existe. Isso permite que você use com eficiência todas as portas no cluster.

Se as portas que você deseja adicionar ao novo domínio de broadcast já estiverem em outro domínio de broadcast, remova as portas desse domínio de broadcast antes de atribuí-las ao novo domínio de broadcast.

Esta tarefa é relevante para o ONTAP 9.0 - 9,7, não para o ONTAP 9.8.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- As portas que pretende adicionar a um domínio de difusão não devem pertencer a outro domínio de difusão.
- As portas que já pertencem a um grupo de interfaces não podem ser adicionadas individualmente a um domínio de broadcast.

Sobre esta tarefa

As regras a seguir se aplicam ao adicionar e remover portas de rede:

Ao adicionar portas…	Ao remover portas…
As portas podem ser portas de rede, VLANs ou grupos de interface (ifgrps).	N/A.
As portas são adicionadas ao grupo de failover definido pelo sistema do domínio de broadcast.	As portas são removidas de todos os grupos de failover no domínio de broadcast.
A MTU das portas é atualizada para o valor MTU definido no domínio de broadcast.	A MTU das portas não muda.
O IPspace das portas é atualizado para o valor IPspace do domínio de broadcast.	As portas são movidas para o espaço IPspace 'padrão' sem atributo de domínio de broadcast.

Se você remover a última porta membro de um grupo de interfaces usando o `network port ifgrp remove-port` comando, isso fará com que a porta do grupo de interfaces seja removida do domínio de broadcast porque uma porta de grupo de interfaces vazia não é permitida em um domínio de broadcast.

Passos

1. Exiba as portas que estão atualmente atribuídas ou não atribuídas a um domínio de broadcast usando o `network port show` comando.
2. Adicionar ou remover portas de rede do domínio de broadcast:

Se você quiser…	Utilizar…

Adicionar portas a um domínio de broadcast	`network port broadcast-domain add-ports`
Remover portas de um domínio de broadcast	`network port broadcast-domain remove-ports`

3. Verifique se as portas foram adicionadas ou removidas do domínio de broadcast:

   `network port show`

Para obter mais informações sobre esses comandos, consulte "Referência do comando ONTAP" .

Exemplos de adição e remoção de portas

O comando a seguir adiciona a porta e0g no cluster de nó-1-01 e a porta e0g no cluster de nó-1-02 para transmitir o domínio bcast1 no IPspace padrão:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

O comando a seguir adiciona duas portas de cluster ao cluster de domínio de broadcast no Cluster IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

O comando a seguir remove a porta e0e no nó cluster1-01 do domínio de broadcast bcast1 no IPspace padrão:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1
-ports cluster-1-01:e0e
```

Domínios de broadcast divididos (ONTAP 9,7 ou anterior)

Você pode modificar um domínio de broadcast existente dividindo-o em dois domínios de broadcast diferentes, com cada domínio de broadcast contendo algumas das portas originais atribuídas ao domínio de broadcast original.

Sobre esta tarefa

- Se as portas estiverem em um grupo de failover, todas as portas em um grupo de failover devem ser divididas.
- Se as portas tiverem LIFs associadas a elas, os LIFs não poderão fazer parte dos intervalos de uma sub-rede.

Passo

Divida um domínio de broadcast em dois domínios de broadcast:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` É o nome do IPspace onde reside o domínio de broadcast.
- `-broadcast-domain` é o nome do domínio de broadcast que será dividido.
- `-new-broadcast-domain` é o nome do novo domínio de broadcast que será criado.
- `-ports` é o nome e a porta do nó a serem adicionados ao novo domínio de broadcast.

Mesclar domínios de broadcast (ONTAP 9 .7 e anteriores)

Você pode mover todas as portas de um domínio de broadcast para um domínio de broadcast existente usando o comando merge.

Esta operação reduz as etapas necessárias se você remover todas as portas de um domínio de broadcast e, em seguida, adicionar as portas a um domínio de broadcast existente.

Passo

Mesclar as portas de um domínio de broadcast em um domínio de broadcast existente:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` É o nome do IPspace onde os domínios de broadcast residem.
- `-broadcast-domain` é o nome do domínio de broadcast que será mesclado.
- `-into-broadcast-domain` é o nome do domínio de broadcast que receberá portas adicionais.

Exemplo

O exemplo a seguir mescla o domínio de broadcast bd-data1 no domínio de broadcast bd-data2:

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

Alterar o valor MTU para portas em um domínio de broadcast (ONTAP 9.7 e anterior)

Você pode modificar o valor MTU de um domínio de broadcast para alterar o valor MTU para todas as portas nesse domínio de broadcast. Isso pode ser feito para suportar alterações de topologia que foram feitas na rede.

Antes de começar

O valor MTU deve corresponder a todos os dispositivos conetados a essa rede de camada 2, exceto para o tráfego de gerenciamento de manipulação de portas e0M.

Sobre esta tarefa

A alteração do valor MTU provoca uma breve interrupção no tráfego nas portas afetadas. O sistema exibe um prompt que você deve responder com y para fazer a alteração da MTU.

Passo

Altere o valor MTU para todas as portas em um domínio de broadcast:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` é o nome do domínio de broadcast.
- `mtu` É o tamanho MTU para pacotes IP; 1500 e 9000 são valores típicos.
- `ipspace` É o nome do IPspace no qual esse domínio de broadcast reside. O espaço IPspace "padrão" é usado a menos que você especifique um valor para esta opção. O comando a seguir altera o MTU para 9000 para todas as portas no domínio de broadcast bcast1:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

Exibir domínios de broadcast (ONTAP 9.7 e anteriores)

Você pode exibir a lista de domínios de broadcast dentro de cada espaço IPspace em um cluster. A saída também mostra a lista de portas e o valor MTU para cada domínio de broadcast.

Passo

Exiba os domínios de broadcast e as portas associadas no cluster:

```
network port broadcast-domain show
```

O comando a seguir exibe todos os domínios de broadcast e portas associadas no cluster:

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        bcast1       1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

O comando a seguir exibe as portas no domínio de broadcast bcast1 que têm um status de atualização de erro, o que indica que a porta não pôde ser atualizada corretamente:

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Default bcast1       1500
                           cluster-1-02:e0g       error
```

Para obter mais informações, consulte "Referência do comando ONTAP" .

Excluir um domínio de broadcast

Se você não precisar mais de um domínio de broadcast, você pode excluí-lo. Isso move as portas associadas a esse domínio de broadcast para o espaço IPspace "padrão".

Antes de começar

Não deve haver sub-redes, interfaces de rede ou SVMs associadas ao domínio de broadcast que você deseja excluir.

Sobre esta tarefa

- O domínio de broadcast "Cluster" criado pelo sistema não pode ser excluído.
- Todos os grupos de failover relacionados ao domínio de broadcast são removidos quando você exclui o domínio de broadcast.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador de sistema para excluir um domínio de broadcast

A opção de exclusão não é exibida quando o domínio de broadcast contém portas ou está associado a uma sub-rede.

Passos

1. Selecione **rede > Visão geral > domínio Broadcast**.
2. Selecione **> Excluir** ao lado do domínio de broadcast que deseja remover.

CLI

Use a CLI para excluir um domínio de broadcast

Passo

Excluir um domínio de broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

O seguinte comando exclui o domínio de broadcast default-1 no IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Grupos e políticas de failover

Visão geral do failover de LIF

Failover de LIF refere-se à migração automática de um LIF para uma porta de rede diferente em resposta a uma falha de link na porta atual do LIF. Este é um componente chave para fornecer alta disponibilidade para as conexões com SVMs. A configuração do failover de LIF envolve a criação de um grupo de failover, a modificação do LIF para usar o grupo de failover e a especificação de uma política de failover.

Um grupo de failover contém um conjunto de portas de rede (portas físicas, VLANs e grupos de interfaces) de um ou mais nós em um cluster. As portas de rede que estão presentes no grupo failover definem os destinos de failover disponíveis para o LIF. Um grupo de failover pode ter gerenciamento de clusters, gerenciamento de nós, clusters e LIFs de dados nas atribuídos a ele.

Quando um LIF é configurado sem um destino de failover válido, ocorre uma interrupção quando o LIF tenta fazer failover. Você pode usar o comando "network interface show -failover" para verificar a configuração de failover.

Quando você cria um domínio de broadcast, um grupo de failover com o mesmo nome é criado automaticamente que contém as mesmas portas de rede. Esse grupo de failover é gerenciado automaticamente pelo sistema, o que significa que, à medida que as portas são adicionadas ou removidas do domínio de broadcast, elas são adicionadas ou removidas automaticamente desse grupo de failover. Isso é fornecido como uma eficiência para administradores que não desejam gerenciar seus próprios grupos de failover.

Crie um grupo de failover

Você cria um grupo de failover de portas de rede para que um LIF possa migrar automaticamente para uma porta diferente se ocorrer uma falha de link na porta atual do LIF. Isto permite que o sistema redirecione o tráfego de rede para outras portas disponíveis no cluster.

Sobre esta tarefa

Use o `network interface failover-groups create` comando para criar o grupo e adicionar portas ao grupo.

- As portas adicionadas a um grupo de failover podem ser portas de rede, VLANs ou grupos de interface (ifgrps).
- Todas as portas adicionadas ao grupo failover devem pertencer ao mesmo domínio de broadcast.
- Uma única porta pode residir em vários grupos de failover.
- Se você tiver LIFs em diferentes VLANs ou domínios de broadcast, configure grupos de failover para cada VLAN ou domínio de broadcast.
- Os grupos de failover não se aplicam a ambientes SAN iSCSI ou FC.

Passo

Criar um grupo de failover:

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* É o nome do SVM que pode usar o grupo failover.
- *`failover_group_name`* é o nome do grupo de failover que você deseja criar.
- *`ports_list`* é a lista de portas que serão adicionadas ao grupo failover. As portas são adicionadas no formato *node_name>:<port_number>*, por exemplo, node1:e0c.

O comando a seguir cria o grupo de failover FG3 para SVM VS3 e adiciona duas portas:

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

Depois de terminar

- Você deve aplicar o grupo failover a um LIF agora que o grupo failover foi criado.
- A aplicação de um grupo de failover que não forneça um destino de failover válido para um LIF resulta em uma mensagem de aviso.

  Se um LIF que não tem um destino de failover válido tentar fazer failover, pode ocorrer uma interrupção.

Configure as configurações de failover em um LIF

Você pode configurar um LIF para fazer failover para um grupo específico de portas de rede aplicando uma política de failover e um grupo de failover ao LIF. Você também pode desativar um LIF de falhar para outra porta.

Sobre esta tarefa

- Quando um LIF é criado, o failover de LIF é ativado por padrão e a lista de portas de destino disponíveis é determinada pelo grupo de failover padrão e pela política de failover com base no tipo de LIF e na política de serviço.

  A partir de 9,5, você pode especificar uma política de serviço para o LIF que define quais serviços de rede podem usar o LIF. Alguns serviços de rede impõem restrições de failover em um LIF.

  > Se a política de serviço de LIF for alterada de uma forma que restrinja ainda mais o failover, a política de failover de LIF é atualizada automaticamente pelo sistema.

- Você pode modificar o comportamento de failover de LIFs especificando valores para os parâmetros -failover-group e -failover-policy no comando Network Interface Modify.
- A modificação de um LIF que faz com que o LIF não tenha um destino de failover válido resulta em uma mensagem de aviso.

  Se um LIF que não tem um destino de failover válido tentar fazer failover, pode ocorrer uma interrupção.

- A partir do ONTAP 9.11,1, em plataformas de array all-flash SAN (ASA), o failover de LIF iSCSI é ativado automaticamente em LIFs iSCSI recém-criadas em VMs de storage recém-criadas.

  Além disso, você pode "Ative manualmente o failover de iSCSI LIF em iSCSI LIFs pré-existentes", significando LIFs que foram criados antes da atualização para o ONTAP 9.11,1 ou posterior.

- A lista a seguir descreve como a configuração de política -failover afeta as portas de destino selecionadas no grupo failover:

  > Para failover de LIF iSCSI, apenas as políticas de failover `local-only` , `sfo-partner-only` e `disabled` são suportadas.

  - `broadcast-domain-wide` aplica-se a todas as portas em todos os nós do grupo failover.
  - `system-defined` Aplica-se apenas às portas no nó inicial do LIF e a um outro nó no cluster, normalmente um parceiro não SFO, se existir.
  - `local-only` Aplica-se apenas às portas no nó inicial do LIF.
  - `sfo-partner-only` Aplica-se apenas às portas no nó inicial do LIF e ao seu parceiro SFO.
  - `disabled` Indica que o LIF não está configurado para failover.

Passos

Configurar as configurações de failover para uma interface existente:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Exemplos de configuração de configurações de failover e desativação de failover

O comando a seguir define a política de failover para broadcast-domain-wide e usa as portas no grupo de failover FG3 como destinos de failover para LIF data1 na SVM VS3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

O seguinte comando desativa o failover para LIF data1 na SVM VS3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

Comandos para gerenciar grupos e políticas de failover

Você pode usar os `network interface failover-groups` comandos para gerenciar grupos de failover. Você usa o `network interface modify` comando para gerenciar os grupos de failover e as políticas de failover aplicadas a um LIF.

Se você quiser…	Use este comando…
Adicionar portas de rede a um grupo de failover	`network interface failover-groups add-targets`
Remova as portas de rede de um grupo de failover	`network interface failover-groups remove-targets`
Modifique as portas de rede em um grupo de failover	`network interface failover-groups modify`
Exibir os grupos de failover atuais	`network interface failover-groups show`

Configurar failover em um LIF	`network interface modify -failover -group -failover-policy`
Exibir o grupo de failover e a política de failover que estão sendo usados por cada LIF	`network interface show -fields failover-group, failover-policy`
Renomeie um grupo de failover	`network interface failover-groups rename`
Excluir um grupo de failover	`network interface failover-groups delete`

Modificar um grupo de failover de modo que ele não forneça um destino de failover válido para qualquer LIF no cluster pode resultar em uma interrupção quando um LIF tenta fazer failover.

Para obter mais informações, consulte as páginas de manual para os `network interface failover-groups` comandos e. `network interface modify`

Sub-redes (somente administradores de cluster)

Descrição geral da sub-rede

As sub-redes permitem alocar blocos ou pools específicos de endereços IP para a configuração da rede ONTAP. Isso permite que você crie LIFs mais facilmente especificando um nome de sub-rede em vez de precisar especificar o endereço IP e os valores de máscara de rede.

Uma sub-rede é criada dentro de um domínio de broadcast e contém um conjunto de endereços IP que pertencem à mesma sub-rede de camada 3. Os endereços IP em uma sub-rede são alocados às portas no domínio de broadcast quando os LIFs são criados. Quando os LIFs são removidos, os endereços IP são retornados ao pool de sub-redes e estão disponíveis para LIFs futuros.

É recomendável que você use sub-redes porque elas facilitam muito o gerenciamento de endereços IP e tornam a criação de LIFs um processo mais simples. Além disso, se você especificar um gateway ao definir uma sub-rede, uma rota padrão para esse gateway será adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.

Crie uma sub-rede

Você pode criar uma sub-rede para alocar blocos específicos de endereços IPv4 ou IPv6 a serem usados posteriormente quando você criar LIFs para o SVM.

Isso permite que você crie LIFs mais facilmente especificando um nome de sub-rede em vez de precisar especificar o endereço IP e os valores de máscara de rede para cada LIF.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

O domínio de broadcast e o IPspace onde você pretende adicionar a sub-rede já devem existir.

Sobre esta tarefa

- Todos os nomes de sub-rede devem ser exclusivos dentro de um espaço IPspace.
- Ao adicionar intervalos de endereços IP a uma sub-rede, você deve garantir que não haja endereços IP sobrepostos na rede para que diferentes sub-redes ou hosts não tentem usar o mesmo endereço IP.
- Se você especificar um gateway ao definir uma sub-rede, uma rota padrão para esse gateway será adicionada automaticamente ao SVM quando um LIF for criado usando essa sub-rede. Se você não usar sub-redes ou se não especificar um gateway ao definir uma sub-rede, precisará usar o `route create` comando para adicionar uma rota ao SVM manualmente.
- O NetApp recomenda a criação de objetos de sub-rede para todas as LIFs em SVMs de dados. Isso é especialmente importante para as configurações do MetroCluster, onde o objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque cada objeto de sub-rede tem um domínio de broadcast associado.

Procedimento

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

A partir do ONTAP 9.12,0, você pode usar o Gerenciador do sistema para criar uma sub-rede.

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Clique + Add para criar uma sub-rede.
3. Nomeie a sub-rede.
4. Especifique o endereço IP da sub-rede.
5. Defina a máscara de sub-rede.
6. Defina o intervalo de endereços IP que compõem a sub-rede.
7. Se útil, especifique um gateway.
8. Selecione o domínio de broadcast ao qual a sub-rede pertence.
9. Salve suas alterações.
   a. Se o endereço IP ou intervalo introduzido já for utilizado por uma interface, é apresentada a seguinte mensagem:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Quando você clica em **OK**, o LIF existente será associado à sub-rede.

CLI

Use a CLI para criar uma sub-rede.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` é o nome da sub-rede da camada 3 que você deseja criar.

  O nome pode ser uma cadeia de texto como "Mgmt" ou pode ser um valor IP de sub-rede específico como 192,0.2,0/24.

- `broadcast_domain_name` é o nome do domínio de broadcast onde a sub-rede residirá.
- `ipspace_name` É o nome do IPspace do qual o domínio de broadcast faz parte.

  O espaço IPspace "padrão" é usado a menos que você especifique um valor para esta opção.

- `subnet_address` É o endereço IP e a máscara da sub-rede; por exemplo, 192,0.2,0/24.
- `gateway_address` é o gateway para a rota padrão da sub-rede; por exemplo, 192,0.2,1.
- `ip_address_list` É a lista, ou intervalo, de endereços IP que serão alocados à sub-rede.

  Os endereços IP podem ser endereços individuais, um intervalo de endereços IP ou uma combinação em uma lista separada por vírgulas.

- O valor `true` pode ser definido para a `-force-update-lif-associations` opção.

  Este comando falhará se algum processador de serviço ou interfaces de rede estiverem usando os endereços IP no intervalo especificado. Definir este valor como verdadeiro associa quaisquer interfaces endereçadas manualmente à sub-rede atual e permite que o comando seja bem-sucedido.

O comando a seguir cria a sub-rede SUB1 no domínio de broadcast default-1 no espaço IPspace padrão. Ele adiciona um endereço IP de sub-rede IPv4 e uma máscara, o gateway e um intervalo de endereços IP:

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

O comando a seguir cria a sub-rede sub2 no padrão de domínio de broadcast no IPspace "padrão". Ele adiciona um intervalo de endereços IPv6:

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

Depois de terminar

Você pode atribuir SVMs e interfaces a um espaço IPspace usando os endereços na sub-rede.

Se você precisar alterar o nome de uma sub-rede existente, use o `network subnet rename` comando.

Adicione ou remova endereços IP de uma sub-rede

Você pode adicionar endereços IP ao criar inicialmente uma sub-rede ou adicionar endereços IP a uma sub-rede que já existe. Você também pode remover endereços IP de uma sub-rede existente. Isso permite alocar apenas os endereços IP necessários para SVMs.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador do sistema para adicionar ou remover endereços IP de ou para uma sub-rede

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Selecione **> Editar** ao lado da sub-rede que deseja alterar.
3. Adicionar ou remover endereços IP.
4. Salve suas alterações.
   a. Se o endereço IP ou intervalo introduzido já for utilizado por uma interface, é apresentada a seguinte mensagem:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Quando você clica em **OK**, o LIF existente será associado à sub-rede.

CLI

Use a CLI para adicionar ou remover endereços IP de ou para uma sub-rede

Sobre esta tarefa

Ao adicionar endereços IP, você receberá um erro se qualquer processador de serviço ou interfaces de rede estiver usando os endereços IP no intervalo que está sendo adicionado. Se pretender associar quaisquer interfaces endereçadas manualmente à sub-rede atual, pode definir a `-force-update-lif-associations` opção como `true`.

Ao remover endereços IP, você receberá um erro se qualquer processador de serviço ou interfaces de rede estiver usando os endereços IP sendo removidos. Se pretender que as interfaces continuem a utilizar os endereços IP após serem removidos da sub-rede, pode definir a `-force-update-lif-associations` opção como `true`.

Passo

Adicionar ou remover endereços IP de uma sub-rede:

Se você quiser…	Use este comando…
Adicione endereços IP a uma sub-rede	extensões de sub-rede
Remover endereços IP de uma sub-rede	remover-intervalos de sub-rede

Para obter mais informações sobre esses comandos, consulte as páginas man.

O comando a seguir adiciona endereços IP 192.0.2.82 a 192.0.2.85 à sub-rede SUB1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

O seguinte comando remove o endereço IP 198.51.100.9 da sub-rede sub3:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

Se o intervalo atual inclui 1 a 10 e 20 a 40, e você deseja adicionar 11 a 19 e 41 a 50 (basicamente permitindo 1 a 50), você pode sobrepor o intervalo existente de endereços usando o seguinte comando. Este comando adiciona apenas os novos endereços e não afeta os endereços existentes:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

Altere as propriedades da sub-rede

Você pode alterar o endereço de sub-rede e o valor da máscara, o endereço de gateway ou o intervalo de endereços IP em uma sub-rede existente.

Sobre esta tarefa

- Ao modificar endereços IP, você deve garantir que não haja endereços IP sobrepostos na rede para que diferentes sub-redes ou hosts não tentem usar o mesmo endereço IP.
- Se você adicionar ou alterar o endereço IP do gateway, o gateway modificado será aplicado a novos SVMs quando um LIF é criado neles usando a sub-rede. Uma rota padrão para o gateway é criada para o SVM se a rota ainda não existir. Talvez seja necessário adicionar manualmente uma nova rota ao SVM ao alterar o endereço IP do gateway.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador do sistema para alterar as propriedades da sub-rede

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Selecione **> Editar** ao lado da sub-rede que deseja alterar.
3. Faça alterações.
4. Salve suas alterações.
   a. Se o endereço IP ou intervalo introduzido já for utilizado por uma interface, é apresentada a seguinte mensagem:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Quando você clica em **OK**, o LIF existente será associado à sub-rede.

CLI

Use a CLI para alterar as propriedades da sub-rede

Passo

Modificar propriedades de sub-rede:

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` é o nome da sub-rede que você deseja modificar.
- `ipspace` É o nome do espaço IPspace onde reside a sub-rede.
- `subnet` é o novo endereço e máscara da sub-rede, se aplicável; por exemplo, 192,0.2,0/24.
- `gateway` é o novo gateway da sub-rede, se aplicável; por exemplo, 192,0.2,1. A introdução de **''** remove a entrada do gateway.
- `ip_ranges` É a nova lista, ou intervalo, de endereços IP que serão alocados à sub-rede, se aplicável. Os endereços IP podem ser endereços individuais, um intervalo ou endereços IP ou uma combinação em uma lista separada por vírgulas. O intervalo especificado aqui substitui os endereços IP existentes.
- `force-update-lif-associations` É necessário quando você altera o intervalo de endereços IP. Você pode definir o valor para **true** para essa opção ao modificar o intervalo de endereços IP. Este comando falhará se algum processador de serviço ou interfaces de rede estiver usando os endereços IP no intervalo especificado. Definir este valor como **True** associa quaisquer interfaces endereçadas manualmente à sub-rede atual e permite que o comando seja bem-sucedido.

O seguinte comando modifica o endereço IP do gateway da sub-rede sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

Exibir sub-redes

Você pode exibir a lista de endereços IP alocados para cada sub-rede dentro de um espaço IPspace. A saída também mostra o número total de endereços IP disponíveis em cada sub-rede e o número de endereços que estão sendo usados atualmente.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com o ONTAP 9.12,0, você pode usar o Gerenciador do sistema para exibir sub-redes

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Veja a lista de sub-redes.

CLI

Use a CLI para exibir sub-redes

Passo

Exiba a lista de sub-redes e os intervalos de endereços IP associados que são usados nessas sub-redes:

```
network subnet show
```

O comando a seguir exibe as sub-redes e as propriedades da sub-rede:

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name   Subnet           Domain    Gateway       Total   Ranges
-----  ---------------- --------- ------------ --------
-----------------------
sub1   192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

Eliminar uma sub-rede

Se você não precisar mais de uma sub-rede e quiser desalocar os endereços IP atribuídos à sub-rede, você pode excluí-la.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador do sistema para excluir uma sub-rede

Passos

1. Selecione **rede > Visão geral > sub-redes**.
2. Selecione **> Excluir** ao lado da sub-rede que deseja remover.
3. Salve suas alterações.

CLI

Use a CLI para excluir uma sub-rede

Sobre esta tarefa

Você receberá um erro se algum processador de serviço ou interfaces de rede estiver usando endereços IP nos intervalos especificados. Se você quiser que as interfaces continuem a usar os endereços IP mesmo depois que a sub-rede é excluída, você pode definir a opção -force-update-lif-associations como true para remover a associação da sub-rede com os LIFs.

Passo

Eliminar uma sub-rede:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

O comando a seguir exclui a sub-rede SUB1 no IPspace ipspace1:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

Crie SVMs

Você precisa criar um SVM para servir dados aos clientes.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve saber qual estilo de segurança o volume raiz da SVM terá.

  Se você pretende implementar uma solução Hyper-V ou SQL Server sobre SMB neste SVM, você deve usar o estilo de segurança NTFS para o volume raiz. Os volumes que contêm ficheiros Hyper-V ou ficheiros de base de dados SQL têm de ser definidos para segurança NTFS no momento em que são criados. Ao definir o estilo de segurança do volume raiz como NTFS, você garante que não crie inadvertidamente volumes de dados UNIX ou mistos de estilo de segurança.

- A partir do ONTAP 9.13,1, é possível definir uma capacidade máxima para uma VM de armazenamento. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

System Manager

Você pode usar o System Manager para criar uma VM de storage.

Passos

1. Selecione **Storage VMs**.
2. Clique + Add em para criar uma VM de armazenamento.
3. Nomeie a VM de storage.
4. Selecione o protocolo de acesso:
   - SMB/CIFS, NFS
   - ISCSI
   - FC
   - NVMe
     i. Se selecionar **Ativar SMB/CIFS**, conclua a seguinte configuração:

Campo ou caixa de verificação	Descrição
Nome do administrador	Especifique o nome de usuário do administrador para a VM de storage SMB/CIFS.
Palavra-passe	Especifique a senha de administrador para a VM de armazenamento SMB/CIFS.
Nome do servidor	Especifique o nome do servidor para a VM de armazenamento SMB/CIFS.
Domínio do ative Directory	Especifique o domínio do diretório ativo para fornecer autenticação de usuário para a VM de storage SMB/CIFS.
Unidade organizacional	Especifique a unidade organizacional no domínio do ative Directory associado ao servidor SMB/CIFS. "Computadores" é o valor padrão, que pode ser modificado.
Criptografa dados enquanto acessa os compartilhamentos na VM de storage	Marque essa caixa de seleção para criptografar dados usando o SMB 3,0 para impedir o acesso não autorizado a arquivos nos compartilhamentos na VM de armazenamento SMB/CIFS.
Domínios	Adicione, remova ou reordene os domínios listados para a VM de armazenamento SMB/CIFS.
Servidores de nomes	Adicione, remova ou reordene os servidores de nomes para a VM de armazenamento SMB/CIFS.

Idioma padrão	Especifica a configuração padrão de codificação de idioma para a VM de armazenamento e seus volumes. Use a CLI para alterar as configurações de volumes individuais em uma VM de armazenamento.
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar NFS**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição
Caixa de verificação permitir acesso do cliente NFS	Marque essa caixa de seleção quando todos os volumes criados na VM de armazenamento NFS devem usar o caminho do volume raiz "/" para montar e percorrer. Adicione regras à política de exportação "default" para permitir a passagem ininterrupta de montagem.

Regras	Clique + Add para criar regras. • Especificação do cliente: Especifique os nomes de host, endereços IP, grupos de rede ou domínios. • Protocolos de acesso: Selecione uma combinação das seguintes opções: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Detalhes de Acesso: Para cada tipo de usuário, especifique o nível de acesso, somente leitura, leitura/gravador ou superusuário. Os tipos de utilizador incluem: ◦ Tudo ◦ Todos (como utilizador anónimo) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5P ◦ NTLM Salve a regra.
Idioma padrão	Especifica a configuração padrão de codificação de idioma para a VM de armazenamento e seus volumes. Use a CLI para alterar as configurações de volumes individuais em uma VM de armazenamento.
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.

Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se selecionar **Ativar iSCSI**, efetue a seguinte configuração:

Campo ou caixa de verificação	Descrição
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar FC**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição
Configurar portas FC	Selecione as interfaces de rede nos nós que você deseja incluir na VM de storage. Duas interfaces de rede por nó são recomendadas.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar NVMe/FC**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição

Configurar portas FC	Selecione as interfaces de rede nos nós que você deseja incluir na VM de storage. Duas interfaces de rede por nó são recomendadas.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Se você selecionar **Ativar NVMe/TCP**, execute a seguinte configuração:

Campo ou caixa de verificação	Descrição
Interface de rede	Para cada interface de rede configurada para a VM de armazenamento, selecione uma sub-rede existente (se existir pelo menos uma) ou especifique **sem uma sub-rede** e preencha os campos **Endereço IP** e **Máscara de sub-rede**. Se for útil, marque a caixa de seleção **Use a mesma máscara de sub-rede e gateway para todas as seguintes interfaces**. Pode permitir que o sistema selecione automaticamente a porta inicial ou selecione manualmente a que pretende utilizar na lista.
Gerenciar conta de administrador	Marque essa caixa de seleção se desejar gerenciar a conta de administrador de VM de armazenamento. Quando selecionado, especifique o nome de usuário, a senha, confirme a senha e indique se deseja adicionar uma interface de rede para gerenciamento de VM de armazenamento.

1. Salve suas alterações.

CLI

Use a CLI do ONTAP para criar uma sub-rede.

Passos

1. Determine quais agregados são candidatos a conter o volume raiz da SVM.

   ```
   storage aggregate show -has-mroot false
   ```

   Você deve escolher um agregado que tenha pelo menos 1 GB de espaço livre para conter o volume raiz. Se você pretende configurar a auditoria nas na SVM, você deve ter um mínimo de 3 GB de espaço livre extra no agregado raiz, com o espaço extra sendo usado para criar o volume de teste de auditoria quando a auditoria estiver ativada.

Se a auditoria nas já estiver habilitada em um SVM existente, o volume de preparo do agregado será criado imediatamente após a criação do agregado ser concluída com sucesso.

2. Registre o nome do agregado no qual você deseja criar o volume raiz do SVM.
3. Se você planeja especificar um idioma ao criar o SVM e não souber o valor a ser usado, identifique e Registre o valor do idioma que deseja especificar:

   ```
   vserver create -language ?
   ```

4. Se você planeja especificar uma política de Snapshot ao criar o SVM e não souber o nome da política, liste as políticas disponíveis e identifique e Registre o nome da política de snapshot que deseja usar:

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. Se você planeja especificar uma política de cota ao criar o SVM e não souber o nome da política, liste as políticas disponíveis e identifique e Registre o nome da política de cota que deseja usar:

   ```
   volume quota policy show -vserver vserver_name
   ```

6. Criar um SVM:

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. Verifique se a configuração SVM está correta.

   ```
   vserver show -vserver vs1
   ```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

Neste exemplo, o comando cria o SVM chamado "VS1" no IPspace "ipspace1". O volume raiz é chamado "VS1_root" e é criado em aggr3 com estilo de segurança NTFS.

A partir do ONTAP 9.13,1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Interfaces lógicas (LIFs)

Visão geral da LIF

Configure a visão geral dos LIFs

Um LIF (interface lógica) representa um ponto de acesso à rede para um nó no cluster. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede.

Um administrador de cluster pode criar, exibir, modificar, migrar, reverter ou excluir LIFs. O administrador do SVM só pode visualizar os LIFs associados ao SVM.

Um LIF é um endereço IP ou WWPN com caraterísticas associadas, como uma política de serviço, uma porta inicial, um nó inicial, uma lista de portas para as quais fazer failover e uma política de firewall. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede.

A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

Os LIFs podem ser hospedados nas seguintes portas:

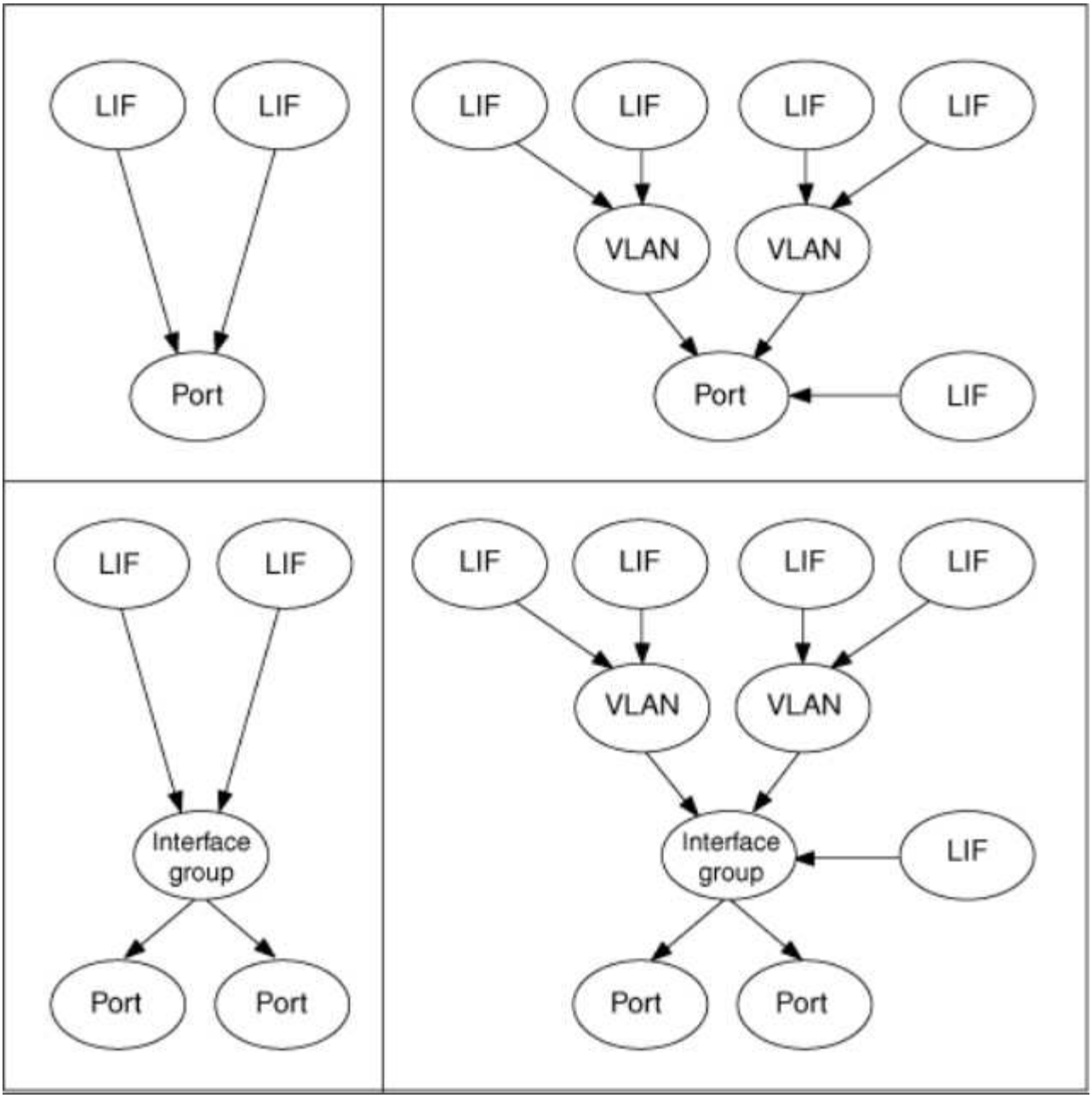
- Portas físicas que não fazem parte dos grupos de interfaces
- Grupos de interfaces
- VLANs
- Portas físicas ou grupos de interface que hospedam VLANs
- Portas IP virtual (VIP)

  A partir do ONTAP 9.5, os LIFs VIP são suportados e são hospedados em portas VIP.

Ao configurar protocolos SAN como FC em um LIF, ele será associado a um WWPN.

"Administração da SAN"

A figura a seguir ilustra a hierarquia de portas em um sistema ONTAP:



Failover de LIF e giveback

Um failover de LIF ocorre quando um LIF passa de seu nó ou porta inicial para o nó ou porta do parceiro de HA. Um failover de LIF pode ser acionado automaticamente pelo ONTAP ou manualmente por um administrador de cluster para certos eventos, como um link físico de Ethernet para baixo ou um nó que sai do quórum de banco de dados replicado (RDB). Quando ocorre um failover de LIF, o ONTAP continua a operação normal no nó do parceiro até que o motivo do failover seja resolvido. Quando o nó inicial ou a porta recupera a integridade, o LIF é revertido do parceiro HA de volta para o nó ou porta inicial. Esta reversão é chamada de giveback.

Para failover de LIF e giveback, as portas de cada nó precisam pertencer ao mesmo domínio de broadcast. Para verificar se as portas relevantes em cada nó pertencem ao mesmo domínio de broadcast, consulte o seguinte:

- ONTAP 9.8 e posterior: "Acessibilidade da porta de reparo"
- ONTAP 9.7 e anteriores: "Adicionar ou remover portas de um domínio de broadcast"

Para LIFs com failover de LIF ativado (automático ou manualmente), o seguinte se aplica:

- Para LIFs usando uma política de serviço de dados, você pode verificar restrições de política de failover:
  - ONTAP 9.6 e posterior: "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"
  - ONTAP 9.5 e anteriores: "Funções de LIF no ONTAP 9.5 e anteriores"
- A reversão automática de LIFs ocorre quando a reversão automática é definida como `true` e quando a porta inicial do LIF está saudável e capaz de hospedar o LIF.
- Em um takeover de nós planejado ou não planejado, o LIF no nó assumido faz failover para o parceiro de HA. A porta em que o LIF falha é determinada pelo Gerenciador de VIF.
- Após a conclusão do failover, o LIF opera normalmente.
- Quando um giveback é iniciado, o LIF volta para seu nó e porta inicial, se a reversão automática estiver definida como `true`.
- Quando um link ethernet é desativado em uma porta que hospeda um ou mais LIFs, o Gerenciador de VIF migra os LIFs da porta para uma porta diferente no mesmo domínio de broadcast. A nova porta pode estar no mesmo nó ou em seu parceiro de HA. Depois que o link for restaurado e se a reversão automática estiver definida como `true`, o Gerenciador de VIF reverte os LIFs de volta ao nó inicial e à porta inicial.
- Quando um nó sai do quórum de banco de dados replicado (RDB), o VIF Manager migra os LIFs do nó de ausência de quorum para seu parceiro de HA. Depois que o nó voltar ao quórum e se a reversão automática estiver definida como `true`, o Gerenciador de VIF reverte os LIFs de volta ao nó inicial e à porta inicial.

Compatibilidade LIF com tipos de portas

LIFs podem ter caraterísticas diferentes para suportar diferentes tipos de portas.

Quando os LIFs de gerenciamento e clusters são configurados na mesma sub-rede, o tráfego de gerenciamento pode ser bloqueado por um firewall externo e as conexões AutoSupport e NTP podem falhar. Você pode recuperar o sistema executando o `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` comando para alternar o LIF entre clusters. No entanto, você deve definir o LIF e o LIF de gerenciamento em diferentes sub-redes para evitar esse problema.

LIF	Descrição
LIF de dados	Um LIF associado a uma máquina virtual de storage (SVM) e usado para comunicação com clientes. Você pode ter vários LIFs de dados em uma porta. Essas interfaces podem migrar ou fazer failover em todo o cluster. É possível modificar um LIF de dados para servir como um LIF de gerenciamento de SVM modificando sua política de firewall para mgmt. As sessões estabelecidas nos servidores NIS, LDAP, ative Directory, WINS e DNS usam LIFs de dados.

LIF de cluster	LIF usado para transportar tráfego entre clusters entre nós em um cluster. As LIFs de cluster sempre devem ser criadas nas portas do cluster. As LIFs de cluster podem fazer failover entre as portas de cluster no mesmo nó, mas não podem ser migradas ou falhadas para um nó remoto. Quando um novo nó se junta a um cluster, os endereços IP são gerados automaticamente. No entanto, se você quiser atribuir endereços IP manualmente aos LIFs de cluster, certifique-se de que os novos endereços IP estejam no mesmo intervalo de sub-rede que os LIFs de cluster existentes.
LIF de gerenciamento de clusters	LIF que fornece uma única interface de gerenciamento para todo o cluster. Um LIF de gerenciamento de cluster pode fazer failover para qualquer nó no cluster. Não pode fazer failover para portas de cluster ou clusters
LIF entre clusters	Um LIF usado para comunicação, backup e replicação entre clusters. É necessário criar um LIF entre clusters em cada nó do cluster antes que uma relação de peering de cluster possa ser estabelecida. Essas LIFs só podem fazer failover para portas no mesmo nó. Eles não podem ser migrados ou falhados para outro nó no cluster.
LIF de gerenciamento de nós	Um LIF que fornece um endereço IP dedicado para gerenciar um nó específico em um cluster. As LIFs de gerenciamento de nós são criadas no momento da criação ou junção do cluster. Esses LIFs são usados para manutenção do sistema, por exemplo, quando um nó fica inacessível do cluster.
LIF VIP	Um LIF VIP é qualquer LIF de dados criado em uma porta VIP. Para saber mais, "Configurar LIFs de IP virtual (VIP)"consulte .

Gerencie o tráfego suportado no ONTAP

Ao longo do tempo, a forma como o ONTAP gerencia o tipo de tráfego suportado nos LIFs mudou.

- O ONTAP 9.5 e versões anteriores usam funções de LIF e serviços de firewall.
- ONTAP 9.6 e versões posteriores usam políticas de serviço LIF:
  - A versão ONTAP 9.5 introduziu políticas de serviço de LIF.
  - O ONTAP 9.6 substituiu as funções de LIF por políticas de serviço de LIF.
  - O ONTAP 9.10,1 substituiu os serviços de firewall por políticas de serviço LIF.

O método que você configura depende da versão do ONTAP que você está usando.

Para saber mais sobre:

- Políticas de firewall, "Comando: Firewall-policy-show"consulte .
- Funções de LIF, "Funções de LIF (ONTAP 9 .5 e anteriores)"consulte a .
- Políticas de serviço de LIF, "LIFs e políticas de serviço (ONTAP 9.6 e posteriores)"consulte .

LIFs e políticas de serviço (ONTAP 9.6 e posteriores)

Você pode atribuir políticas de serviço (em vez de funções de LIF ou políticas de firewall) a LIFs que determinam o tipo de tráfego suportado para os LIFs. As políticas de serviço

definem uma coleção de serviços de rede suportados por um LIF. O ONTAP fornece um conjunto de políticas de serviço integradas que podem ser associadas a um LIF.

Você pode exibir as políticas de serviço e seus detalhes usando o seguinte comando:
`network interface service-policy show`

Os recursos que não estão vinculados a um serviço específico usarão um comportamento definido pelo sistema para selecionar LIFs para conexões de saída.

Os aplicativos em um LIF com uma política de serviço vazia podem se comportar inesperadamente.

Políticas de serviço para SVMs do sistema

O SVM admin e qualquer SVM do sistema contêm políticas de serviço que podem ser usadas para LIFs nesse SVM, incluindo gerenciamento e LIFs entre clusters. Essas políticas são criadas automaticamente pelo sistema quando um IPspace é criado.

A tabela a seguir lista as políticas internas para LIFs em SVMs do sistema a partir do ONTAP 9.12,1. Para outras versões, exiba as políticas de serviço e seus detalhes usando o seguinte comando:

`network interface service-policy show`

Política	Serviços incluídos	Função equivalente	Descrição
padrão-clusters	núcleo entre clusters, gerenciamento-https	entre clusters	Usado por LIFs que transportam tráfego entre clusters. Observação: O Service entre clusters-core está disponível no ONTAP 9.5 com o nome da política de serviços de rede.
default-route-announce	gestão-bgp	-	Usado por LIFs que transportam conexões de pares BGP Nota: Disponível a partir do ONTAP 9.5 com o nome net-route-announce Service policy.
gerenciamento padrão	management-core, management-https, management-http, management-ssh, management-AutoSupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	node-mgmt ou cluster-mgmt	Use essa política de gerenciamento de escopo do sistema para criar LIFs de gerenciamento com escopo de nó e cluster pertencentes a um SVM do sistema. Esses LIFs podem ser usados para conexões de saída para servidores DNS, AD, LDAP ou NIS, bem como algumas conexões adicionais para suportar aplicativos executados em nome de todo o sistema. A partir do ONTAP 9.12,1, você pode usar o `management-log-forwarding` serviço para controlar quais LIFs são usados para encaminhar logs de auditoria para um servidor syslog remoto.

A tabela a seguir lista os serviços que os LIFs podem usar em um SVM do sistema a partir do ONTAP 9.11,1:

Serviço	Limitações de failover	Descrição
núcleo entre clusters	somente nó inicial	Serviços básicos entre clusters
núcleo de gerenciamento	-	Serviços de gerenciamento central
gestão-ssh	-	Serviços para acesso de gerenciamento SSH
http de gerenciamento	-	Serviços para acesso de gerenciamento HTTP
gerenciamento-https	-	Serviços para acesso de gerenciamento HTTPS
management-AutoSupport	-	Serviços relacionados com a publicação de cargas úteis AutoSupport
gestão-bgp	apenas porta inicial	Serviços relacionados com interações entre pares BGP
backup-controle ndmp	-	Serviços para controles de backup NDMP
gestão-ems	-	Serviços para acesso de mensagens de gerenciamento
gerenciamento-ntp-cliente	-	Introduzido no ONTAP 9.10,1. Serviços para acesso de cliente NTP.
servidor de gerenciamento ntp	-	Introduzido no ONTAP 9.10,1. Serviços para acesso de gerenciamento de servidor NTP
gerenciamento-portmap	-	Serviços para gerenciamento de portmap
management-rsh-server	-	Serviços para gerenciamento de servidores rsh
management-snmp-server	-	Serviços para gerenciamento de servidores SNMP
management-tetelnet-server	-	Serviços para gerenciamento de servidores telnet
encaminhamento de logs de gerenciamento	-	Introduzido no ONTAP 9.12,1. Serviços para encaminhamento de logs de auditoria

Políticas de serviço para SVMs de dados

Todas as SVMs de dados contêm políticas de serviço que podem ser usadas por LIFs nesse SVM.

A tabela a seguir lista as políticas internas para LIFs em SVMs de dados a partir do ONTAP 9.11,1. Para outras versões, exiba as políticas de serviço e seus detalhes usando o seguinte comando:

```
network interface service-policy show
```

Política	Serviços incluídos	Protocolo de dados equivalente	Descrição
gerenciamento padrão	management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nenhum	Use essa política de gerenciamento com escopo da SVM para criar LIFs de gerenciamento de SVM de propriedade de um data SVM. Esses LIFs podem ser usados para fornecer acesso SSH ou HTTPS aos administradores do SVM. Quando necessário, esses LIFs podem ser usados para conexões de saída para servidores DNS, AD, LDAP ou NIS externos.
blocos de dados padrão	data-core, data-iscsi	iscsi	Usado por LIFs que transportam tráfego de dados SAN orientado a blocos. A partir do ONTAP 9.10,1, a política "default-data-blocks" está obsoleta. Em vez disso, utilize a política de serviço "Default-data-iscsi".
arquivos-dados-padrão	data-fpolicy-client, data-dns-server, data-FlexCache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Use a política arquivos de dados padrão para criar LIFs nas que suportam protocolos de dados baseados em arquivos. Às vezes, há apenas um LIF presente no SVM, portanto, essa política permite que o LIF seja usado para conexões de saída a um servidor DNS, AD, LDAP ou NIS externo. Você pode remover esses serviços dessa política se preferir que essas conexões utilizem apenas LIFs de gerenciamento.
padrão-data-iscsi	data-core, data-iscsi	iscsi	Usado por LIFs que transportam tráfego de dados iSCSI.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Usado por LIFs que transportam tráfego de dados NVMe/TCP.

A tabela a seguir lista os serviços que podem ser usados em um SVM de dados, juntamente com quaisquer restrições que cada serviço impõe à política de failover de LIF a partir do ONTAP 9.11,1:

Serviço	Restrições de failover	Descrição
gestão-ssh	-	Serviços para acesso de gerenciamento SSH
http de gerenciamento	-	Introduzido nos Serviços ONTAP 9.10,1 para acesso de gerenciamento HTTP

gerenciamento-https	-	Serviços para acesso de gerenciamento HTTPS
gerenciamento-portmap	-	Serviços para acesso ao gerenciamento de portmap
management-snmp-server	-	Introduzido nos Serviços ONTAP 9.10,1 para acesso de gestão de servidores SNMP
núcleo de dados	-	Serviços de dados básicos
data-nfs	-	Serviço de dados NFS
data-cifs	-	Serviço de dados CIFS
data-FlexCache	-	Serviço de dados FlexCache
dados-iscsi	Apenas porta inicial para AFF/FAS; apenas parceiro sfo para ASA	Serviço de dados iSCSI
backup-controle ndmp	-	Introduzido no ONTAP 9.10,1 Backup NDMP controla o serviço de dados
servidor-dns de dados	-	Introduzido no serviço de dados do servidor DNS ONTAP 9.10,1
data-fpolicy-client	-	Serviço de dados de política de triagem de arquivos
data-nvme-tcp	apenas porta inicial	Introduzido no serviço de dados TCP NVMe ONTAP 9.10,1
data-s3-server	-	Serviço de dados de servidor Simple Storage Service (S3)

Você deve estar ciente de como as políticas de serviço são atribuídas aos LIFs em SVMs de dados:

- Se um SVM de dados for criado com uma lista de serviços de dados, as políticas de serviço incorporadas "arquivos de dados padrão" e "blocos de dados padrão" nesse SVM serão criadas usando os serviços especificados.
- Se um SVM de dados for criado sem especificar uma lista de serviços de dados, as políticas de serviço incorporadas "default-data-files" e "default-data-blocks" nesse SVM serão criadas usando uma lista padrão de serviços de dados.

  A lista de serviços de dados padrão inclui os serviços iSCSI, NFS, NVMe, SMB e FlexCache.

- Quando um LIF é criado com uma lista de protocolos de dados, uma política de serviço equivalente aos protocolos de dados especificados é atribuída ao LIF.
- Se não existir uma política de serviço equivalente, é criada uma política de serviço personalizada.

- Quando um LIF é criado sem uma política de serviço ou lista de protocolos de dados, a política de serviço de arquivos de dados padrão é atribuída ao LIF por padrão.

Serviço de data center

O serviço data-core permite que componentes que usaram LIFs anteriormente com a função de dados funcionem como esperado em clusters que foram atualizados para gerenciar LIFs usando políticas de serviço em vez de funções LIF (que são depreciadas no ONTAP 9.6).

Especificar o data-core como um serviço não abre portas no firewall, mas o serviço deve ser incluído em qualquer política de serviço em um data SVM. Por exemplo, a política de serviço default-data-files contém os seguintes serviços por padrão:

- núcleo de dados
- data-nfs
- data-cifs
- data-FlexCache

O serviço de núcleo de dados deve ser incluído na política para garantir que todos os aplicativos que usam o LIF funcionem conforme esperado, mas os outros três serviços podem ser removidos, se desejado.

Serviço de LIF do lado do cliente

A partir do ONTAP 9.10,1, o ONTAP fornece serviços de LIF do lado do cliente para várias aplicações. Esses serviços fornecem controle sobre quais LIFs são usados para conexões de saída em nome de cada aplicativo.

Os novos serviços a seguir fornecem aos administradores controle sobre quais LIFs são usados como endereços de origem para determinados aplicativos.

Serviço	Restrições da SVM	Descrição
gestão-ad-cliente	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente do ative Directory para conexões de saída a um servidor AD externo.
management-dns-client	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente DNS para conexões de saída a um servidor DNS externo.
gerenciamento-ldap-cliente	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente LDAP para conexões de saída a um servidor LDAP externo.
management-nis-client	-	A partir do ONTAP 9.11,1, o ONTAP fornece serviço de cliente NIS para conexões de saída a um servidor NIS externo.
gerenciamento-ntp-cliente	apenas sistema	A partir do ONTAP 9.10,1, o ONTAP fornece serviço de cliente NTP para conexões de saída a um servidor NTP externo.

data-fpolicy-client	somente dados	A partir do ONTAP 9.8, o ONTAP fornece serviço de cliente para conexões FPolicy de saída.

Cada um dos novos serviços é incluído automaticamente em algumas das políticas de serviço incorporadas, mas os administradores podem removê-los das políticas incorporadas ou adicioná-los a políticas personalizadas para controlar quais LIFs são usados para conexões de saída em nome de cada aplicativo.

Funções de LIF (ONTAP 9 .5 e anteriores)

LIFs com papéis diferentes têm caraterísticas diferentes. Uma função LIF determina o tipo de tráfego suportado pela interface, juntamente com as regras de failover aplicáveis, as restrições de firewall que estão em vigor, a segurança, o balanceamento de carga e o comportamento de roteamento para cada LIF. Um LIF pode ter qualquer uma das seguintes funções: Cluster, gerenciamento de cluster, dados, clusters, gerenciamento de nós e undef (undefined). O papel undef é usado para LIFs BGP.

A partir do ONTAP 9.6, as funções de LIF são obsoletas. Você deve especificar políticas de serviço para LIFs em vez de uma função. Não é necessário especificar uma função LIF ao criar um LIF com uma política de serviço.

Segurança LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Requer sub-rede IP privada?	Não	Sim	Não	Não	Não
Requer rede segura?	Não	Sim	Não	Não	Sim
Política de firewall predefinida	Muito restritivo	Completamente aberto	Média	Média	Muito restritivo
O firewall é personalizável?	Sim	Não	Sim	Sim	Sim

Failover de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters

Comportamento padrão	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF e em um nó de parceiro não-SFO	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF	Qualquer porta no mesmo grupo de failover	Apenas as portas no mesmo grupo de failover que estão no nó inicial do LIF
É personalizável?	Sim	Não	Sim	Sim	Sim

Encaminhamento de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Quando é necessária uma rota predefinida?	Quando os clientes ou o controlador de domínio estão em sub-rede IP diferente	Nunca	Quando qualquer um dos tipos principais de tráfego requer acesso a uma sub-rede IP diferente	Quando o administrador estiver se conetando a partir de outra sub-rede IP	Quando outras LIFs de clusters estão em uma sub-rede IP diferente
Quando é necessária uma rota estática para uma sub-rede IP específica?	Raro	Nunca	Raro	Raro	Quando os nós de outro cluster têm suas LIFs de clusters em sub-redes IP diferentes
Quando é necessária uma rota de host estática para um servidor específico?	Para ter um dos tipos de tráfego listados em LIF de gerenciamento de nós, passe por um LIF de dados em vez de um LIF de gerenciamento de nós. Isso requer uma alteração de firewall correspondente.	Nunca	Raro	Raro	Raro

Rebalanceamento de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
DNS: Usar como servidor DNS?	Sim	Não	Não	Não	Não
DNS: Exportar como zona?	Sim	Não	Não	Não	Não

Tipos de tráfego primário de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Tipos de tráfego principais	Servidor NFS, servidor CIFS, cliente NIS, ative Directory, LDAP, WINS, cliente e servidor DNS, servidor iSCSI e FC	Sem brilho	Servidor SSH, servidor HTTPS, cliente NTP, SNMP, cliente AutoSupport, cliente DNS, carregamento de atualizações de software	Servidor SSH, servidor HTTPS	Replicação entre clusters

Gerenciar LIFs

Configurar políticas de serviço de LIF

Você pode configurar políticas de serviço de LIF para identificar um único serviço ou uma lista de serviços que usarão um LIF.

Crie uma política de serviço para LIFs

Você pode criar uma política de serviço para LIFs. Você pode atribuir uma política de serviço a um ou mais LIFs, permitindo assim que o LIF transporte tráfego para um único serviço ou uma lista de serviços.

Você precisa de Privileges avançado para executar o `network interface service-policy create` comando.

Sobre esta tarefa

Serviços incorporados e políticas de serviço estão disponíveis para gerenciar dados e tráfego de gerenciamento em SVMs de dados e do sistema. A maioria dos casos de uso é satisfeita usando uma política de serviço integrada em vez de criar uma política de serviço personalizada.

Você pode modificar essas políticas de serviço integradas, se necessário.

Passos

1. Veja os serviços disponíveis no cluster:

```
network interface service show
```

Os serviços representam os aplicativos acessados por um LIF, bem como os aplicativos servidos pelo cluster. Cada serviço inclui zero ou mais portas TCP e UDP nas quais o aplicativo está escutando.

Estão disponíveis os seguintes serviços de gerenciamento e dados adicionais:

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. Veja as políticas de serviço que existem no cluster:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Criar uma política de serviço:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- "service_name" especifica uma lista de serviços que devem ser incluídos na política.
- "IP_address/mask" especifica a lista de máscaras de sub-rede para endereços que têm permissão para acessar os serviços na política de serviço. Por padrão, todos os serviços especificados são adicionados com uma lista de endereços padrão permitidos de 0,0.0,0/0, que permite o tráfego de todas as sub-redes. Quando uma lista de endereços permitidos não padrão é fornecida, LIFs usando a diretiva são configurados para bloquear todas as solicitações com um endereço de origem que não corresponde a nenhuma das máscaras especificadas.

  O exemplo a seguir mostra como criar uma política de serviço de dados, *svm1_data_policy*, para um SVM que inclui serviços *NFS* e *SMB*:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  O exemplo a seguir mostra como criar uma política de serviços entre clusters:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Verifique se a política de serviço foi criada.

```
cluster1::> network interface service-policy show
```

A saída a seguir mostra as políticas de serviço que estão disponíveis:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

Depois de terminar

Atribua a política de serviço a um LIF no momento da criação ou modificando um LIF existente.

Atribua uma política de serviço a um LIF

Você pode atribuir uma política de serviço a um LIF no momento da criação do LIF ou modificando o LIF. Uma política de serviço define a lista de serviços que podem ser usados com o LIF.

Sobre esta tarefa

Você pode atribuir políticas de serviço para LIFs nos SVMs de administração e de dados.

Passo

Dependendo de quando você deseja atribuir a política de serviço a um LIF, execute uma das seguintes ações:

Se você é…	Atribuir a política de serviço…
Criando um LIF	Crie -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> ((-address <IP_address> -netmask <IP_address>) -sub-rede-name <subnet_name>) -Service-policy <service_policy_name>
Modificação de um LIF	interface de rede modificar -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

Ao especificar uma política de serviço para um LIF, não é necessário especificar o protocolo de dados e a função para o LIF. A criação de LIFs especificando a função e os protocolos de dados também é suportada.

Uma política de serviço só pode ser usada por LIFs no mesmo SVM que você especificou ao criar a política de serviço.

Exemplos

O exemplo a seguir mostra como modificar a política de serviço de um LIF para usar a política de serviço de gerenciamento padrão:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Comandos para gerenciar políticas de serviço LIF

Use os `network interface service-policy` comandos para gerenciar políticas de serviço LIF.

Antes de começar

Modificar a política de serviço de um LIF em uma relação do SnapMirror ativa interrompe a programação de replicação. Se você converter um LIF entre clusters (ou vice-versa), essas alterações não serão replicadas para o cluster com peering. Para atualizar o cluster de pares depois de modificar a política de serviço LIF, execute primeiro a `snapmirror abort` operação e ressincronize a relação de replicaçãodepois .

Se você quiser…	Use este comando…
Criar uma política de serviço (Privileges avançado necessário)	`network interface service-policy create`

Se você quiser…	Use este comando…
Adicionar uma entrada de serviço adicional a uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy add-service`
Clonar uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy clone`
Modificar uma entrada de serviço em uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy modify-service`
Remover uma entrada de serviço de uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy remove-service`
Renomear uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy rename`
Excluir uma política de serviço existente (Privileges avançado necessário)	`network interface service-policy delete`
Restaurar uma política de serviço incorporada ao seu estado original (Privileges avançado necessário)	`network interface service-policy restore-defaults`
Exibir políticas de serviço existentes	`network interface service-policy show`

Criar um LIF (interface de rede)

Um SVM fornece dados a clientes por meio de uma ou mais interfaces lógicas de rede (LIFs). Você deve criar LIFs nas portas que deseja usar para acessar dados. Um LIF (interface de rede) é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

Prática recomendada

As portas de switch conetadas ao ONTAP devem ser configuradas como portas de borda de spanning-tree para reduzir atrasos durante a migração de LIF.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- A porta de rede física ou lógica subjacente deve ter sido configurada para o estado de funcionamento administrativo.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o System Manager ou o `network subnet create` comando.

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Não é possível atribuir protocolos nas e SAN ao mesmo LIF.

  Os protocolos compatíveis são SMB, NFS, FlexCache, iSCSI e FC; iSCSI e FC não podem ser combinados com outros protocolos. No entanto, os protocolos SAN baseados em nas e Ethernet podem estar presentes na mesma porta física.

  - Você não deve configurar LIFs que transportam tráfego SMB para reverter automaticamente para seus nós domésticos. Esta recomendação é obrigatória se o servidor SMB for hospedar uma solução para operações ininterruptas com Hyper-V ou SQL Server sobre SMB.
- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Todos os serviços de mapeamento de nomes e resolução de nomes de host usados por um SVM, como DNS, NIS, LDAP e ative Directory, devem ser acessíveis a partir de pelo menos um LIF que manipula o tráfego de dados do SVM.
- Um tráfego entre nós que lida com LIF não deve estar na mesma sub-rede que um tráfego de gerenciamento de manipulação de LIF ou um tráfego de dados de manipulação de LIF.
- Criar um LIF que não tenha um destino de failover válido resulta em uma mensagem de aviso.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster:
  - Gerenciador do sistema: Começando com ONTAP 9.12,0, visualize o throughput na grade de interface de rede.
  - CLI: Use o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível avançado de privilégio).
- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

  A partir do ONTAP 9.4, o FC-NVMe é compatível. Se você estiver criando um LIF FC-NVMe, deve estar ciente do seguinte:

  - O protocolo NVMe precisa ser compatível com o adaptador FC no qual o LIF é criado.
  - O FC-NVMe pode ser o único protocolo de dados em LIFs de dados.
- Um tráfego de gerenciamento de manipulação de LIF deve ser configurado para cada máquina virtual de storage (SVM) que suporte SAN.
- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- Somente um LIF NVMe que manipula o tráfego de dados pode ser configurado por SVM.
- Quando você cria uma interface de rede com uma sub-rede, o ONTAP seleciona automaticamente um endereço IP disponível na sub-rede selecionada e o atribui à interface de rede. Você pode alterar a sub-rede se houver mais de uma sub-rede, mas não pode alterar o endereço IP.
- Ao criar (adicionar) um SVM, para uma interface de rede, não é possível especificar um endereço IP que esteja no intervalo de uma sub-rede existente. Você receberá um erro de conflito de sub-rede. Esse problema ocorre em outros fluxos de trabalho para uma interface de rede, como criar ou modificar interfaces de rede entre clusters nas configurações de SVM ou configurações de cluster.

- A partir do ONTAP 9.10,1, os `network interface` comandos CLI incluem um `-rdma-protocols` parâmetro para NFS sobre configurações RDMA. A criação de interfaces de rede para NFS em configurações RDMA é suportada no Gerenciador de sistemas a partir do ONTAP 9.12,1. Para obter mais informações, Configure o LIFS para NFS através do RDMAconsulte .
- A partir do ONTAP 9.11,1, o failover automático de LIF iSCSI está disponível em plataformas de array all-flash SAN (ASA).

  O failover de LIF iSCSI é ativado automaticamente (a política de failover é definida como `sfo-partner-only` e o valor de reversão automática é definido como `true`) em iSCSI LIFs recém-criados se não existirem LIFs iSCSI na SVM especificada ou se todas as LIFs iSCSI existentes na SVM especificada já estiverem habilitadas com failover de LIF iSCSI.

  Se após a atualização para o ONTAP 9.11,1 ou posterior, você tiver LIFs iSCSI existentes em uma SVM que não tenha sido habilitada com o recurso de failover de LIF iSCSI e criar novas LIFs iSCSI na mesma SVM, os novos LIFs iSCSI assumirão a mesma política de failover (`disabled`) das LIFs iSCSI existentes na SVM.

  "Failover de LIF iSCSI para plataformas ASA"

A partir do ONTAP 9.7, o ONTAP escolhe automaticamente a porta inicial de um LIF, desde que pelo menos um LIF já exista na mesma sub-rede nesse espaço. O ONTAP escolhe uma porta inicial no mesmo domínio de broadcast que outros LIFs nessa sub-rede. Você ainda pode especificar uma porta inicial, mas ela não é mais necessária (a menos que ainda não existam LIFs nessa sub-rede no espaço IPspace especificado).

A partir do ONTAP 9.12,0, o procedimento a seguir depende da interface que você usa — Gerenciador de sistema ou CLI:

System Manager

Use o System Manager para adicionar uma interface de rede

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. + Add Selecione .
3. Selecione uma das seguintes funções de interface:
   a. Dados
   b. Entre clusters
   c. Gerenciamento de SVM
4. Selecione o protocolo:
   a. SMB/CIFS E NFS
   b. ISCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Nomeie o LIF ou aceite o nome gerado a partir de suas seleções anteriores.
6. Aceite o nó inicial ou utilize a lista pendente para selecionar um.
7. Se pelo menos uma sub-rede estiver configurada no espaço IPspace do SVM selecionado, a lista suspensa de sub-rede será exibida.
   a. Se você selecionar uma sub-rede, escolha-a na lista suspensa.
   b. Se você continuar sem uma sub-rede, o menu suspenso domínio de broadcast será exibido:
      i. Especifique o endereço IP. Se o endereço IP estiver a ser utilizado, é apresentada uma mensagem de aviso.
      ii. Especifique uma máscara de sub-rede.
8. Selecione a porta inicial no domínio de transmissão, automaticamente (recomendado) ou selecionando uma no menu suspenso. O controle de porta inicial é exibido com base no domínio de broadcast ou na seleção de sub-rede.
9. Salve a interface de rede.

CLI

Use a CLI para criar um LIF

Passos

1. Determine quais portas de domínio de broadcast você deseja usar para o LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

2. Verifique se a sub-rede que você deseja usar para os LIFs contém endereços IP não utilizados suficientes.

   `network subnet show -ipspace` *`ipspace1`*

3. Crie um ou mais LIFs nas portas que você deseja usar para acessar dados.

   > O NetApp recomenda a criação de objetos de sub-rede para todas as LIFs em SVMs de dados. Isso é especialmente importante para as configurações do MetroCluster, onde o objeto de sub-rede permite que o ONTAP determine destinos de failover no cluster de destino porque cada objeto de sub-rede tem um domínio de broadcast associado. Para obter instruções, "Crie uma sub-rede"consulte .

   ```
   network interface create -vserver _SVM_name_ -lif _lif_name_
   -service-policy _service_policy_name_ -home-node _node_name_ -home
   -port port_name {-address _IP_address_ - netmask _Netmask_value_ |
   -subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
   {true|false}
   ```

   - `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

     Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a opção -auto-revert.

   - `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
   - Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
   - Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
   - Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
   - `-auto-revert` Permite que você especifique se um LIF de dados é automaticamente revertido

para seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `true` dependendo das políticas de gerenciamento de rede em seu ambiente.

- `-service-policy` A partir do ONTAP 9.5, você pode atribuir uma política de serviço para o LIF com a `-service-policy` opção. Quando uma política de serviço é especificada para um LIF, a política é usada para criar uma função padrão, política de failover e lista de protocolos de dados para o LIF. No ONTAP 9.5, as políticas de serviço são suportadas apenas para serviços de pares entre clusters e BGP. No ONTAP 9.6, você pode criar políticas de serviço para vários serviços de dados e gerenciamento.
- `-data-protocol` Permite criar um LIF compatível com os protocolos FCP ou NVMe/FC. Esta opção não é necessária ao criar um IP LIF.

4. **Opcional**: Atribua um endereço IPv6 na opção -address:

   a. Use o comando Network ndp prefix show para exibir a lista de prefixos RA aprendidos em várias interfaces.

      O `network ndp prefix show` comando está disponível no nível de privilégio avançado.

   b. Use o formato `prefix::id` para construir o endereço IPv6 manualmente.

      `prefix` é o prefixo aprendido em várias interfaces.

   Para derivar o `id`, escolha um número hexadecimal aleatório de 64 bits.

5. Verifique se a configuração da interface LIF está correta.

   `network interface show -vserver vs1`

```
          Logical    Status     Network          Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- ---------------- --------- -------
----
vs1
           lif1       up/up      10.0.0.128/24   node1     e0d
true
```

6. Verifique se a configuração do grupo de failover é a desejada.

   `network interface show -failover -vserver` *vs1*

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	ping de rede
Endereço IPv6	rede ping6

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

O comando a seguir cria um LIF NVMe/FC e especifica o `nvme-fc` protocolo de dados:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modificar um LIF

Você pode modificar um LIF alterando os atributos, como nó inicial ou nó atual, status administrativo, endereço IP, máscara de rede, política de failover, política de firewall e política de serviço. Você também pode alterar a família de endereços de um LIF de IPv4 para IPv6.

Sobre esta tarefa

- Ao modificar o status administrativo de um LIF para baixo, todos os bloqueios NFSv4 pendentes são mantidos até que o status administrativo do LIF seja retornado para cima.

  Para evitar conflitos de bloqueio que podem ocorrer quando outros LIFs tentam acessar os arquivos bloqueados, você deve mover os clientes NFSv4 para um LIF diferente antes de definir o status administrativo para baixo.

- Não é possível modificar os protocolos de dados usados por um LIF FC. No entanto, você pode modificar os serviços atribuídos a uma política de serviço ou alterar a política de serviço atribuída a um IP LIF.

  Para modificar os protocolos de dados usados por um LIF FC, você deve excluir e recriar o LIF. Para fazer alterações de política de serviço em um IP LIF, há uma breve interrupção enquanto as atualizações ocorrem.

- Não é possível modificar o nó inicial ou o nó atual de um LIF de gerenciamento com escopo de nó.
- Ao usar uma sub-rede para alterar o endereço IP e o valor da máscara de rede para um LIF, um endereço IP é alocado da sub-rede especificada; se o endereço IP anterior do LIF for de uma sub-rede diferente, o endereço IP será retornado a essa sub-rede.
- Para modificar a família de endereços de um LIF de IPv4 a IPv6, você deve usar a notação de dois pontos para o endereço IPv6 e adicionar um novo valor para o `-netmask-length` parâmetro.
- Não é possível modificar os endereços IPv6 locais de link auto-configurados.
- A modificação de um LIF que faz com que o LIF não tenha um destino de failover válido resulta em uma mensagem de aviso.

  Se um LIF que não tem um destino de failover válido tentar fazer failover, pode ocorrer uma interrupção.

- A partir do ONTAP 9.5, você pode modificar a política de serviço associada a um LIF.

  No ONTAP 9.5, as políticas de serviço são suportadas apenas para serviços de pares entre clusters e BGP. No ONTAP 9.6, você pode criar políticas de serviço para vários serviços de dados e gerenciamento.

- A partir do ONTAP 9.11,1, o failover automático de LIF iSCSI está disponível em plataformas de array all-flash SAN (ASA).

  Para LIFs iSCSI pré-existentes, ou seja, LIFs criadas antes da atualização para o 9.11.1 ou posterior, você pode modificar a política de failover para "Ativar failover automático de LIF iSCSI"o .

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Começando com ONTAP 9.12,0, você pode usar o Gerenciador de sistema para editar uma interface de rede

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione **> Editar** ao lado da interface de rede que deseja alterar.
3. Altere uma ou mais definições da interface de rede. Para obter detalhes, "Crie um LIF"consulte .
4. Salve suas alterações.

CLI

Use a CLI para modificar um LIF

Passos

1. Modifique os atributos de um LIF usando o `network interface modify` comando.

   O exemplo a seguir mostra como modificar o endereço IP e a máscara de rede do LIF datalif2 usando um endereço IP e o valor da máscara de rede da sub-rede client1_sub:

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   O exemplo a seguir mostra como modificar a política de serviço de um LIF.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

2. Verifique se os endereços IP estão acessíveis.

Se você estiver usando…	Então use…
Endereços IPv4	`network ping`
Endereços IPv6	`network ping6`

Migração de um LIF

Você pode ter que migrar um LIF para uma porta diferente no mesmo nó ou em um nó diferente dentro do cluster, se a porta estiver com defeito ou precisar de manutenção. A migração de um LIF é semelhante ao failover de LIF, mas a migração de LIF é uma operação manual, enquanto o failover de LIF é a migração automática de um LIF em resposta a uma falha de link na porta de rede atual do LIF.

Antes de começar

- Um grupo de failover deve ter sido configurado para os LIFs.
- O nó de destino e as portas devem estar operacionais e ter acesso à mesma rede que a porta de origem.

Sobre esta tarefa

- Os LIFs BGP residem na porta inicial e não podem ser migrados para nenhum outro nó ou porta.
- Você deve migrar LIFs hospedadas nas portas pertencentes a uma NIC para outras portas no cluster, antes de remover a NIC do nó.
- Você deve executar o comando para migração de um cluster LIF do nó onde o cluster LIF está hospedado.
- Um LIF com escopo de nó, como um LIF de gerenciamento com escopo de nó, LIF de cluster e LIF entre clusters, não pode ser migrado para um nó remoto.
- Quando um NFSv4 LIF é migrado entre nós, um atraso de até 45 segundos resulta antes que o LIF esteja disponível em uma nova porta.

  Para contornar esse problema, use NFSv4,1 onde nenhum atraso é encontrado.

- É possível migrar iSCSI LIFs em plataformas de array SAN all-flash (ASA) executando o ONTAP 9.11,1 ou posterior.

  A migração de iSCSI LIFs está limitada a portas no nó inicial ou no parceiro de HA.

- Se a sua plataforma não for uma plataforma ASA (All-Flash SAN Array) executando o ONTAP versão 9.11.1 ou posterior, não será possível migrar LIFs iSCSI de um nó para outro.

  Para contornar essa restrição, você deve criar um iSCSI LIF no nó de destino. Saiba mais "A criar iSCSI LIFs"sobre .

- Se você quiser migrar um LIF (interface de rede) para NFS por RDMA, você deve garantir que a porta de destino seja compatível com RoCE. Você deve estar executando o ONTAP 9.10,1 ou posterior para migrar um LIF com a CLI ou o ONTAP 9.12,1 para migrar usando o Gerenciador de sistema. No System Manager, depois de selecionar sua porta de destino compatível com RoCE, marque a caixa ao lado de **usar portas RoCE** para concluir a migração com êxito. Saiba mais "Configurando LIFs para NFS em RDMA"sobre o .
- As operações de descarga de cópia do VMware VAAI falham ao migrar a LIF de origem ou de destino. Saiba mais sobre a cópia off-load:
  - "Ambientes NFS"
  - "AMBIENTES SAN"

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para migrar uma interface de rede

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione ⋮ **> migrar** ao lado da interface de rede que deseja alterar.

   Para um iSCSI LIF, na caixa de diálogo **Migrate Interface**, selecione o nó de destino e a porta do parceiro de HA.

   Se pretender migrar o iSCSI LIF permanentemente, selecione a caixa de verificação. O iSCSI LIF deve estar offline antes de ser migrado permanentemente. Além disso, uma vez que um iSCSI LIF é migrado permanentemente, ele não pode ser desfeito. Não há opção de reversão.

3. Clique em **Migrate**.
4. Salve suas alterações.

CLI

Use a CLI para migrar um LIF

Passo

Dependendo se você deseja migrar um LIF específico ou todos os LIFs, execute a ação apropriada:

Se você quiser migrar…	Digite o seguinte comando…
Um LIF específico	`network interface migrate`
Todas as LIFs de gerenciamento de cluster e dados em um nó	`network interface migrate-all`
Todos os LIFs fora de um porto	`network interface migrate-all -node <node> -port <port>`

O exemplo a seguir mostra como migrar um LIF `datalif1` nomeado no SVM `vs0` para a porta `e0d` no `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

O exemplo a seguir mostra como migrar todos os LIFs de gerenciamento de cluster e dados do nó atual (local):

```
network interface migrate-all -node local
```

Reverter um LIF para sua porta inicial

Você pode reverter um LIF para sua porta inicial depois que ele falha ou é migrado para uma porta diferente manualmente ou automaticamente. Se a porta inicial de um determinado LIF não estiver disponível, o LIF permanece em sua porta atual e não é revertido.

Sobre esta tarefa

- Se você administrativamente levar a porta inicial de um LIF para o estado up antes de definir a opção de reversão automática, o LIF não será retornado à porta inicial.
- O LIF não reverte automaticamente a menos que o valor da opção "auto-revert" esteja definido como verdadeiro.
- Você deve garantir que a opção "reversão automática" esteja ativada para que os LIFs revertam para suas portas residenciais.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para reverter uma interface de rede para sua porta inicial

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione ⋮ **> Reverter** ao lado da interface de rede que deseja alterar.
3. Selecione **Revert** para reverter uma interface de rede para sua porta inicial.

CLI

Use a CLI para reverter um LIF para sua porta inicial

Passo

Reverter um LIF para sua porta inicial manualmente ou automaticamente:

Se você quiser reverter um LIF para sua porta inicial…	Em seguida, digite o seguinte comando…
Manualmente	`network interface revert -vserver vserver_name -lif lif_name`
Automaticamente	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

ONTAP 9.8 e posterior: Recupere de um cluster LIF configurado incorretamente

Um cluster não pode ser criado quando a rede do cluster é cabeada para um switch, mas nem todas as portas configuradas no Cluster IPspace podem alcançar as outras portas configuradas no Cluster IPspace.

Sobre esta tarefa

Em um cluster comutado, se uma interface de rede de cluster (LIF) estiver configurada na porta errada ou se

uma porta de cluster estiver conetada à rede errada, o `cluster create` comando poderá falhar com o seguinte erro:

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Os resultados do `network port show` comando podem mostrar que várias portas são adicionadas ao Cluster IPspace porque estão conetadas a uma porta configurada com um cluster LIF. No entanto, os resultados do `network port reachability show -detail` comando revelam quais portas não têm conetividade entre si.

Para recuperar de um cluster LIF configurado em uma porta que não é acessível às outras portas configuradas com cluster LIFs, execute as seguintes etapas:

Passos

1. Redefina a porta inicial do LIF do cluster para a porta correta:

   ```
   network port modify -home-port
   ```

2. Remova as portas que não têm LIFs de cluster configuradas a partir do domínio de broadcast do cluster:

   ```
   network port broadcast-domain remove-ports
   ```

3. Crie o cluster:

   ```
   cluster create
   ```

Resultado

Ao concluir a criação do cluster, o sistema deteta a configuração correta e coloca as portas nos domínios de broadcast corretos.

Eliminar um LIF

Você pode excluir uma interface de rede (LIF) que não seja mais necessária.

Antes de começar

Os LIFs a serem excluídos não devem estar em uso.

Passos

1. Marque os LIFs que você deseja excluir como administrativamente para baixo usando o seguinte comando:

   ```
   network interface modify -vserver vserver_name -lif lif_name -status
   -admin down
   ```

2. Use o `network interface delete` comando para excluir um ou todos os LIFs:

Se você quiser excluir…	Introduza o comando …
Um LIF específico	`network interface delete -vserver vserver_name -lif lif_name`
Todos os LIFs	`network interface delete -vserver vserver_name -lif *`

O comando a seguir exclui o LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Use o `network interface show` comando para confirmar que o LIF é excluído.

Configurar LIFs ONTAP virtual IP (VIP)

Alguns data centers de última geração usam mecanismos de rede de camada 3 (IP) que exigem falha de LIFs nas sub-redes. O ONTAP suporta LIFs de dados de IP virtual (VIP) e o protocolo de roteamento associado, protocolo de gateway de borda (BGP), para atender aos requisitos de failover dessas redes de próxima geração.

Sobre esta tarefa

Um LIF de dados VIP é um LIF que não faz parte de qualquer sub-rede e é acessível a partir de todas as portas que hospedam um LIF BGP no mesmo espaço IPspace. Um LIF de dados VIP elimina a dependência de um host em interfaces de rede individuais. Como vários adaptadores físicos transportam o tráfego de dados, toda a carga não se concentra em um único adaptador e na sub-rede associada. A existência de um LIF de dados VIP é anunciada para roteadores peer através do protocolo de roteamento, Border Gateway Protocol (BGP).

Os LIFs de dados VIP oferecem as seguintes vantagens:

- Portabilidade de LIF além de um domínio de broadcast ou sub-rede: LIFs de dados VIP podem falhar em qualquer sub-rede na rede, anunciando a localização atual de cada LIF de dados VIP para roteadores através do BGP.
- Taxa de transferência agregada: Os LIFs de dados VIP podem oferecer suporte a taxa de transferência agregada que excede a largura de banda de qualquer porta individual porque os LIFs VIP podem enviar ou receber dados de várias sub-redes ou portas simultaneamente.

Configurar o protocolo de gateway de borda (BGP)

Antes de criar LIFs VIP, você deve configurar o BGP, que é o protocolo de roteamento usado para anunciar a existência de um LIF VIP para roteadores peer.

A partir do ONTAP 9.9,1, o VIP fornece automação de rota padrão opcional usando grupos de pares BGP para simplificar a configuração.

O ONTAP tem uma maneira simples de aprender rotas padrão usando os pares BGP como roteadores de próximo salto quando o par BGP está na mesma sub-rede. Para usar o recurso, defina o `-use-peer-as`

`-next-hop` atributo como `true`. Por padrão, esse atributo é `false`.

Se você tiver rotas estáticas configuradas, elas ainda serão preferidas sobre essas rotas padrão automatizadas.

Antes de começar

O roteador peer deve ser configurado para aceitar uma conexão BGP do BGP LIF para o ASN (número de sistema autônomo) configurado.

> O ONTAP não processa quaisquer anúncios de rota de entrada a partir do router; por conseguinte, deve configurar o router ponto-a-ponto para não enviar quaisquer atualizações de rota para o cluster. Isso reduz o tempo necessário para que a comunicação com o peer se torne totalmente funcional e reduz o uso de memória interna no ONTAP.

Sobre esta tarefa

Configurar o BGP envolve, opcionalmente, criar uma configuração BGP, criar um BGP LIF e criar um grupo de pares BGP. O ONTAP cria automaticamente uma configuração BGP padrão com valores padrão quando o primeiro grupo de pares BGP é criado em um determinado nó.

Um BGP LIF é usado para estabelecer sessões BGP TCP com roteadores peer. Para um roteador peer, um BGP LIF é o próximo salto para alcançar um VIP LIF. O failover está desativado para o BGP LIF. Um grupo de pares BGP anuncia as rotas VIP para todos os SVMs no IPspace usado pelo grupo de pares. O IPspace usado pelo grupo de pares é herdado do BGP LIF.

A partir do ONTAP 9.16,1, a autenticação MD5 é suportada em grupos de pares BGP para proteger sessões BGP. Quando o MD5 está ativado, as sessões de BGP só podem ser estabelecidas e processadas entre pares autorizados, evitando possíveis interrupções da sessão por um ator não autorizado.

Os seguintes campos foram adicionados `network bgp peer-group create` aos comandos e `network bgp peer-group modify`:

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Esses parâmetros permitem configurar um grupo de pares BGP com uma assinatura MD5 para maior segurança. Os seguintes requisitos aplicam-se ao uso da autenticação MD5.1X:

- Só é possível especificar o `-md5-secret` parâmetro quando o `-md5-enabled` parâmetro estiver definido como `true`.
- O IPsec deve estar ativado globalmente antes de poder ativar a autenticação BGP MD5. O BGP LIF não é necessário para ter uma configuração IPsec ativa. "Configurar a segurança IP (IPsec) através da criptografia por fio"Consulte a .
- A NetApp recomenda que você configure o MD5 no roteador antes de configurá-lo no controlador ONTAP.

A partir de ONTAP 9.9,1, estes campos foram adicionados:

- `-asn` Ou `-peer-asn` (valor de 4 bytes) o atributo em si não é novo, mas agora usa um inteiro de 4 bytes.
- `-med`
- `-use-peer-as-next-hop`

Pode fazer seleções de rota avançadas com suporte Multi-Exit discriminator (MED) para a priorização de

caminho. MED é um atributo opcional na mensagem de atualização do BGP que informa aos roteadores para selecionar a melhor rota para o tráfego. O MED é um número inteiro de 32 bits não assinado (0 - 4294967295); valores mais baixos são preferidos.

A partir de ONTAP 9.8, esses campos foram adicionados ao `network bgp peer-group` comando:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Esses atributos BGP permitem que você configure os atributos caminho COMO e comunidade para o grupo de pares BGP.

> Embora o ONTAP ofereça suporte aos atributos BGP acima, os roteadores não precisam honrá-los. A NetApp recomenda fortemente que você confirme quais atributos são suportados pelo seu roteador e configure os grupos de pares BGP de acordo. Para obter detalhes, consulte a documentação BGP fornecida pelo seu roteador.

Passos

1. Inicie sessão no nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Opcional: Crie uma configuração BGP ou modifique a configuração BGP padrão do cluster executando uma das seguintes ações:

   a. Criar uma configuração BGP:

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

   > - O `-routerid` parâmetro aceita um valor de 32 bits decimal pontilhado que só precisa ser exclusivo dentro de um DOMÍNIO AS. A NetApp recomenda que você use o endereço IP de gerenciamento de nós (v4) para `<router_id>` o qual garanta a exclusividade.
   > - Embora o ONTAP BGP suporte números ASN de 32 bits, apenas a notação decimal padrão é suportada. Notação ASN pontilhada, como 65000,1 em vez de 4259840001 para um ASN privado, não é suportada.

   Amostra com um ASN de 2 bytes:

   ```
   network bgp config create -node node1 -asn 65502 -holdtime 180
   -routerid 1.1.1.1
   ```

   Amostra com um ASN de 4 bytes:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. Modifique a configuração padrão do BGP:

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` Especifica o número ASN. Começando com ONTAP 9.8, o ASN para BGP suporta um inteiro não negativo de 2 bytes. Este é um número de 16 bits (1 a 65534 valores disponíveis). Começando com ONTAP 9.9,1, o ASN para BGP suporta um inteiro não negativo de 4 bytes (1 a 4294967295). O ASN padrão é 65501. O ASN 23456 é reservado para estabelecimento de sessão ONTAP com pares que não anunciam capacidade ASN de 4 bytes.
- `<hold_time>` especifica o tempo de espera em segundos. O valor padrão é 180s.

> O ONTAP suporta apenas um global `<asn_number>`, , `<hold_time>` e `<router_id>`, mesmo que você configure o BGP para vários IPspaces. O BGP e todas as informações de roteamento IP são completamente isolados dentro de um espaço IPspace. Um espaço IPspace é equivalente a uma instância de roteamento e encaminhamento virtual (VRF).

3. Crie um BGP LIF para o SVM do sistema:

   Para o IPspace padrão, o nome do SVM é o nome do cluster. Para IPspaces adicionais, o nome SVM é idêntico ao nome IPspace.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

   Você pode usar a `default-route-announce` política de serviço para o BGP LIF ou qualquer política de serviço personalizado que contenha o serviço "Management-bgp".

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. Crie um grupo de pares BGP que seja usado para estabelecer sessões BGP com os roteadores peer remotos e configurar as informações de rota VIP que são anunciadas aos roteadores peer:

   Exemplo 1: Crie um grupo de pares sem uma rota padrão automática

   Neste caso, o administrador precisa criar uma rota estática para o peer BGP.

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

Exemplo 2: Crie um grupo de pares com uma rota padrão automática

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Exemplo 3: Crie um grupo de pares com o MD5 ativado

a. Ativar IPsec:

```
security ipsec config modify -is-enabled true
```

b. Crie o grupo de pares BGP com o MD5 ativado:

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Exemplo usando uma chave sextavada:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657400
```

Exemplo usando uma cadeia de carateres:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

Depois de criar o grupo de pares BGP, uma porta ethernet virtual (começando com v0a..v0z,v1a…) é listada quando você executa o `network port show` comando. A MTU desta interface é sempre relatada em 1500. A MTU real usada para tráfego é derivada da porta física (BGP LIF), que é determinada quando o tráfego é enviado.

Crie um IP virtual (VIP) data LIF

A existência de um LIF de dados VIP é anunciada para roteadores peer através do protocolo de roteamento, Border Gateway Protocol (BGP).

Antes de começar

- O grupo de pares BGP deve ser configurado e a sessão BGP para o SVM no qual o LIF deve ser criado deve estar ativa.
- Uma rota estática para o roteador BGP ou qualquer outro roteador na sub-rede BGP LIF deve ser criada para qualquer tráfego VIP de saída para o SVM.
- Você deve ativar o roteamento multipath para que o tráfego VIP de saída possa utilizar todas as rotas disponíveis.

  Se o roteamento multipath não estiver habilitado, todo o tráfego VIP de saída será de uma única interface.

Passos

1. Crie um LIF de dados VIP:

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   Uma porta VIP será selecionada automaticamente se você não especificar a porta inicial com o `network interface create` comando.

   Por padrão, o LIF de dados VIP pertence ao domínio de broadcast criado pelo sistema chamado 'VIP', para cada espaço IPspace. Não é possível modificar o domínio de transmissão VIP.

   Um LIF de dados VIP é acessível simultaneamente em todas as portas que hospedam um LIF BGP de um

IPspace. Se não houver uma sessão de BGP ativa para o SVM do VIP no nó local, o LIF de dados VIP fará failover para a próxima porta VIP no nó que tiver uma sessão de BGP estabelecida para esse SVM.

2. Verifique se a sessão BGP está no status up para o SVM do LIF de dados VIP:

```
network bgp vserver-status show

Node        Vserver  bgp status
          ----------  -------- ---------
          node1       vs1      up
```

Se o status do BGP for `down` para o SVM em um nó, o LIF de dados VIP fará o failover para um nó diferente no qual o status do BGP está ativo para o SVM. Se o status do BGP estiver `down` em todos os nós, o LIF de dados VIP não pode ser hospedado em qualquer lugar e tem status de LIF como inativo.

Comandos para gerenciar o BGP

A partir do ONTAP 9.5, você usa os `network bgp` comandos para gerenciar as sessões BGP no ONTAP.

Gerenciar a configuração do BGP

Se você quiser…	Use este comando…
Crie uma configuração BGP	`network bgp config create`
Modificar a configuração do BGP	`network bgp config modify`
Eliminar configuração BGP	`network bgp config delete`
Apresentar a configuração BGP	`network bgp config show`
Exibe o status do BGP para o SVM do VIP LIF	`network bgp vserver-status show`

Gerenciar valores padrão BGP

Se você quiser…	Use este comando…
Modificar valores padrão BGP	`network bgp defaults modify`
Exibir valores padrão BGP	`network bgp defaults show`

Gerenciar grupos de pares BGP

Se você quiser…	Use este comando…
Crie um grupo de pares BGP	`network bgp peer-group create`
Modificar um grupo de pares BGP	`network bgp peer-group modify`
Excluir um grupo de pares BGP	`network bgp peer-group delete`
Exibir informações de grupos de pares BGP	`network bgp peer-group show`
Renomeie um grupo de pares BGP	`network bgp peer-group rename`

Gerencie grupos de pares BGP com MD5

A partir do ONTAP 9.16,1, você pode ativar ou desativar a autenticação MD5 em um grupo de pares BGP existente.

> Se você ativar ou desativar o MD5 em um grupo de pares BGP existente, a conexão BGP será encerrada e recriada para aplicar as alterações de configuração do MD5.

Se você quiser…	Use este comando…
Ative MD5 em um grupo de pares BGP existente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Desative o MD5 em um grupo de pares BGP existente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Informações relacionadas

"Referência do comando ONTAP"

Equilibre as cargas da rede

Visão geral da rede de equilíbrio

Você pode configurar seu cluster para atender solicitações de clientes a partir de LIFs adequadamente carregados. Isso resulta em uma utilização mais equilibrada de LIFs e portas, o que, por sua vez, permite um melhor desempenho do cluster.

O balanceamento de carga DNS ajuda a selecionar um LIF de dados carregado adequadamente e equilibrar o tráfego de rede do usuário em todas as portas disponíveis (físicas, grupos de interfaces e VLANs).

Com o balanceamento de carga DNS, LIFs são associados à zona de balanceamento de carga de um SVM. Um servidor DNS em todo o site é configurado para encaminhar todas as solicitações DNS e retornar o LIF menos carregado com base no tráfego de rede e na disponibilidade dos recursos da porta (uso da CPU, taxa de transferência, conexões abertas, etc.). O balanceamento de carga DNS oferece os seguintes benefícios:

- Novas conexões de clientes equilibradas entre os recursos disponíveis.
- Nenhuma intervenção manual é necessária para decidir quais LIFs usar ao montar um SVM específico.
- O balanceamento de carga DNS suporta NFSv3, NFSv4, NFSv4,1, SMB 2,0, SMB 2,1, SMB 3,0 e S3.

Como o balanceamento de carga DNS funciona

Os clientes montam um SVM especificando um endereço IP (associado a um LIF) ou um nome de host (associado a vários endereços IP). Por padrão, os LIFs são selecionados pelo servidor DNS em todo o site de forma round-robin, que equilibra a carga de trabalho em todos os LIFs.

O balanceamento de carga round-robin pode resultar em sobrecarga de alguns LIFs, então você tem a opção de usar uma zona de balanceamento de carga DNS que lida com a resolução de nome de host em um SVM. Usando uma zona de balanceamento de carga DNS, garante um melhor equilíbrio das novas conexões de clientes entre os recursos disponíveis, levando a um melhor desempenho do cluster.

Uma zona de balanceamento de carga DNS é um servidor DNS dentro do cluster que avalia dinamicamente a carga em todos os LIFs e retorna um LIF carregado adequadamente. Em uma zona de balanceamento de carga, o DNS atribui um peso (métrica), com base na carga, a cada LIF.

Cada LIF é atribuído um peso com base na carga da porta e na utilização da CPU do seu nó inicial. LIFs que estão em portas menos carregadas têm uma maior probabilidade de serem retornadas em uma consulta DNS. Os pesos também podem ser atribuídos manualmente.

Crie uma zona de balanceamento de carga DNS

Você pode criar uma zona de balanceamento de carga DNS para facilitar a seleção dinâmica de um LIF com base na carga, ou seja, o número de clientes montados em um LIF. Você pode criar uma zona de balanceamento de carga ao criar um LIF de dados.

Antes de começar

O encaminhador DNS no servidor DNS de todo o site deve ser configurado para encaminhar todas as solicitações para a zona de balanceamento de carga para os LIFs configurados.

O artigo da base de conhecimento "Como configurar o balanceamento de carga DNS no modo Cluster"no site de suporte da NetApp contém mais informações sobre a configuração do balanceamento de carga DNS usando encaminhamento condicional.

Sobre esta tarefa

- Qualquer LIF de dados pode responder a consultas DNS para um nome de zona de balanceamento de carga DNS.
- Uma zona de balanceamento de carga DNS deve ter um nome exclusivo no cluster e o nome da zona deve atender aos seguintes requisitos:
  - Não deve exceder 256 carateres.
  - Deve incluir pelo menos um período.
  - O primeiro e o último caráter não devem ser um período ou qualquer outro caráter especial.
  - Não pode incluir espaços entre carateres.
  - Cada rótulo no nome DNS não deve exceder 63 carateres.

    Um rótulo é o texto que aparece antes ou depois do período. Por exemplo, a zona DNS chamada storage.company.com tem três rótulos.

Passo

Use o `network interface create` comando com a `dns-zone` opção para criar uma zona de balanceamento de carga DNS.

Se a zona de balanceamento de carga já existir, o LIF é adicionado a ela. Para obter mais informações sobre o comando, consulte "Referência do comando ONTAP" .

O exemplo a seguir demonstra como criar uma zona de balanceamento de carga DNS chamada storage.company.com ao criar o LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Adicione ou remova um LIF de uma zona de balanceamento de carga

Você pode adicionar ou remover um LIF da zona de balanceamento de carga DNS de uma máquina virtual (SVM). Você também pode remover todos os LIFs simultaneamente de uma zona de balanceamento de carga.

Antes de começar

- Todas as LIFs em uma zona de balanceamento de carga devem pertencer ao mesmo SVM.
- Um LIF pode fazer parte de apenas uma zona de balanceamento de carga DNS.
- Os grupos de failover para cada sub-rede devem ter sido configurados, se os LIFs pertencerem a diferentes sub-redes.

Sobre esta tarefa

Um LIF que está no status administrativo inativo é temporariamente removido da zona de balanceamento de carga DNS. Quando o LIF retorna ao status administrativo up, o LIF é adicionado automaticamente à zona de balanceamento de carga DNS.

Passo

Adicione um LIF ou remova um LIF de uma zona de balanceamento de carga:

Se você quiser…	Digite…
Adicione um LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* Exemplo: `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`
Remova um único LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone none` Exemplo: `network interface modify -vserver vs1 -lif data1 -dns-zone none`
Remova todas as LIFs	`network interface modify -vserver` *`vserver_name`* `-lif * -dns-zone none` Exemplo: `network interface modify -vserver vs0 -lif * -dns-zone none` Você pode remover um SVM de uma zona de balanceamento de carga removendo todas as LIFs na SVM dessa zona.

Configurar serviços DNS (ONTAP 9.8 e posterior)

Você deve configurar serviços DNS para o SVM antes de criar um servidor NFS ou SMB. Geralmente, os servidores de nomes DNS são os servidores DNS integrados ao ative Directory para o domínio em que o servidor NFS ou SMB se juntará.

Sobre esta tarefa

Os servidores DNS integrados ao ative Directory contêm os registos de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio. Se o SVM não conseguir localizar os servidores LDAP e os controladores de domínio do ative Directory, a configuração do servidor NFS ou SMB falhará.

Os SVMs usam o banco de dados ns-switch de serviços de nome de hosts para determinar quais serviços de nome usar e em qual ordem ao procurar informações sobre hosts. Os dois serviços de nomes suportados para o banco de dados hosts são arquivos e dns.

Você deve garantir que o dns seja uma das fontes antes de criar o servidor SMB.

> Para exibir as estatísticas dos serviços de nome DNS para o processo mgwd e o processo SecD, use a IU Estatística.

Passos

1. Determine qual é a configuração atual para o banco de dados de serviços de nome do host. Neste exemplo, o banco de dados do serviço de nomes de hosts usa as configurações padrão.

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. Execute as seguintes ações, se necessário.

   a. Adicione o serviço de nomes DNS ao banco de dados do serviço de nomes hosts na ordem desejada ou reordene as fontes.

      Neste exemplo, o banco de dados hosts é configurado para usar arquivos DNS e locais nessa ordem.

      `vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files`

   b. Verifique se a configuração dos serviços de nome está correta.

      `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Name Service Source Order: dns, files
   ```

3. Configurar serviços DNS.

   `vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51`

O comando vserver services name-service dns create executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

4. Verifique se a configuração DNS está correta e se o serviço está ativado.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Valide o status dos servidores de nomes.

```
vserver services name-service dns check -vserver vs1
```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configurar DNS dinâmico na SVM

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS de um servidor NFS ou SMB no DNS, você deverá configurar o DNS dinâmico (DDNS) no SVM.

Antes de começar

Os serviços de nomes DNS devem ser configurados no SVM. Se você estiver usando o DDNS seguro, use servidores de nomes DNS integrados ao ative Directory e crie um servidor NFS ou SMB ou uma conta do ative Directory para o SVM.

Sobre esta tarefa

O nome de domínio totalmente qualificado (FQDN) especificado deve ser exclusivo:

O nome de domínio totalmente qualificado (FQDN) especificado deve ser exclusivo:

- Para NFS, o valor especificado em `-vserver-fqdn` como parte `vserver services name-service dns dynamic-update` do comando torna-se o FQDN registrado para os LIFs.
- Para SMB, os valores especificados como o nome NetBIOS do servidor CIFS e o nome de domínio totalmente qualificado do servidor CIFS tornam-se o FQDN registrado para os LIFs. Isso não é configurável no ONTAP. No cenário a seguir, o FQDN de LIF é "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Para evitar uma falha de configuração de um FQDN SVM que não esteja em conformidade com as regras RFC para atualizações DDNS, use um nome FQDN compatível com RFC. Para obter mais informações, "RFC 1123"consulte .

Passos

1. Configurar o DDNS na SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates
   ```

   ```
   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Asteriscos não podem ser usados como parte do FQDN personalizado. Por exemplo, `*.netapp.com` não é válido.

2. Verifique se a configuração DDNS está correta:

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Configurar serviços DNS (ONTAP 9.7 e anteriores)

Você deve configurar serviços DNS para o SVM antes de criar um servidor NFS ou SMB. Geralmente, os servidores de nomes DNS são os servidores DNS integrados ao ative Directory para o domínio em que o servidor NFS ou SMB se juntará.

Sobre esta tarefa

Os servidores DNS integrados ao ative Directory contêm os registos de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio. Se o SVM não conseguir localizar os servidores LDAP e os controladores de domínio do ative Directory, a configuração do servidor NFS ou SMB falhará.

Os SVMs usam o banco de dados ns-switch de serviços de nome de hosts para determinar quais serviços de nome usar e em qual ordem ao procurar informações sobre hosts. Os dois serviços de nomes suportados para o banco de dados hosts são `files` e `dns`.

Você deve garantir `dns` que seja uma das fontes antes de criar o servidor SMB.

Para exibir as estatísticas dos serviços de nome DNS para o processo mgwd e o processo SecD, use a IU Estatística.

Passos

1. Determine qual é a configuração atual para o `hosts` banco de dados de serviços de nome.

   Neste exemplo, o banco de dados do serviço de nomes de hosts usa as configurações padrão.

   `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

   ```
                       Vserver: vs1
   Name Service Switch Database: hosts
      Name Service Source Order: files, dns
   ```

2. Execute as seguintes ações, se necessário.

   a. Adicione o serviço de nomes DNS ao banco de dados do serviço de nomes hosts na ordem desejada ou reordene as fontes.

      Neste exemplo, o banco de dados hosts é configurado para usar arquivos DNS e locais nessa ordem.

   `vserver services name-service *ns-switch* modify -vserver *vs1* -database *hosts* -sources *dns,files*`

   a. Verifique se a configuração dos serviços de nome está correta.

      `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

3. Configurar serviços DNS.

   `vserver services name-service dns create -vserver *vs1* -domains *example.com,example2.com* -name-servers *10.0.0.50,10.0.0.51*`

   O comando vserver services `name-service dns create` executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

4. Verifique se a configuração DNS está correta e se o serviço está ativado.

```
           Vserver: vs1
           Domains: example.com, example2.com Name
           Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
  Maximum Attempts: 1
```

5. Valide o status dos servidores de nomes.

   `vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
-------  -----------  ------  ----------------------
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configurar DNS dinâmico na SVM

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS de um servidor NFS ou SMB no DNS, você deverá configurar o DNS dinâmico (DDNS) no SVM.

Antes de começar

Os serviços de nomes DNS devem ser configurados no SVM. Se você estiver usando o DDNS seguro, use servidores de nomes DNS integrados ao ative Directory e crie um servidor NFS ou SMB ou uma conta do ative Directory para o SVM.

Sobre esta tarefa

O nome de domínio totalmente qualificado (FQDN) especificado deve ser exclusivo:

- Para NFS, o valor especificado em `-vserver-fqdn` como parte `vserver services name-service dns dynamic-update` do comando torna-se o FQDN registrado para os LIFs.
- Para SMB, os valores especificados como o nome NetBIOS do servidor CIFS e o nome de domínio totalmente qualificado do servidor CIFS tornam-se o FQDN registrado para os LIFs. Isso não é configurável no ONTAP. No cenário a seguir, o FQDN de LIF é "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Para evitar uma falha de configuração de um FQDN SVM que não esteja em conformidade com as regras RFC para atualizações DDNS, use um nome FQDN compatível com RFC. Para obter mais informações, "RFC 1123"consulte .

Passos

1. Configurar o DDNS na SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates
   ```

   ```
   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Asteriscos não podem ser usados como parte do FQDN personalizado. Por exemplo, `*.netapp.com` não é válido.

2. Verifique se a configuração DDNS está correta:

   ```
   vserver services name-service dns dynamic-update show
   ```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Configurar serviços DNS dinâmicos

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS de um servidor NFS ou SMB no DNS, você deverá configurar o DNS dinâmico (DDNS) no SVM.

Antes de começar

Os serviços de nomes DNS devem ser configurados no SVM. Se você estiver usando o DDNS seguro, use servidores de nomes DNS integrados ao ative Directory e crie um servidor NFS ou SMB ou uma conta do ative Directory para o SVM.

Sobre esta tarefa

O FQDN especificado deve ser exclusivo.

> Para evitar uma falha de configuração de um FQDN SVM que não esteja em conformidade com as regras RFC para atualizações DDNS, use um nome FQDN compatível com RFC.

Passos

1. Configurar o DDNS na SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Asteriscos não podem ser usados como parte do FQDN personalizado. Por exemplo, `*.netapp.com` não é válido.

2. Verifique se a configuração DDNS está correta:

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Resolução do nome do host

Visão geral da resolução do nome do host

O ONTAP deve ser capaz de traduzir nomes de host para endereços IP numéricos, a fim de fornecer acesso aos clientes e aos serviços de acesso. Você deve configurar máquinas virtuais de armazenamento (SVMs) para usar serviços de nome locais ou externos para resolver informações de host. O ONTAP suporta a configuração de um servidor DNS externo ou a configuração do arquivo hosts local para resolução de nome de host.

Ao usar um servidor DNS externo, você pode configurar o DNS dinâmico (DDNS), que envia automaticamente informações DNS novas ou alteradas do seu sistema de armazenamento para o servidor DNS. Sem atualizações de DNS dinâmicas, você deve adicionar manualmente informações de DNS (nome de DNS e endereço IP) aos servidores DNS identificados quando um novo sistema é colocado on-line ou quando as informações de DNS existentes forem alteradas. Este processo é lento e propenso a erros. Durante a

recuperação de desastres, a configuração manual pode resultar em um longo tempo de inatividade.

Configurar DNS para resolução de nome de host

Você usa o DNS para acessar fontes locais ou remotas para obter informações sobre o host. Você deve configurar o DNS para acessar uma ou ambas as fontes.

O ONTAP deve ser capaz de procurar informações de host para fornecer acesso adequado aos clientes. Você deve configurar serviços de nomes para permitir que o ONTAP acesse serviços DNS locais ou externos para obter as informações do host.

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX.

Configurar uma SVM e LIFs de dados para resolução de nome de host usando um servidor DNS externo

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os nomes de host são resolvidos usando servidores DNS externos.

Antes de começar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

Consulte Configurar serviços DNS dinâmicos para obter mais informações sobre como configurar o DNS dinâmico no SVM.

Passos

1. Habilite o DNS na SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> O `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Valide o status dos servidores de nomes usando o `vserver services name-service dns check`

comando.

```
vserver services name-service dns check -vserver vs1.example.com
                                      Name Server
Vserver             Name Server       Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50         up           Response time (msec): 2
vs1.example.com     10.0.0.51         up           Response time (msec): 2
```

Para obter informações sobre políticas de serviço relacionadas ao DNS, "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"consulte .

Configure a Tabela de interrutores do serviço de nomes para resolução de nome de host

Você deve configurar a tabela de switch de serviço de nomes corretamente para permitir que o ONTAP consulte o serviço de nomes local ou externo para recuperar informações do host.

Antes de começar

Você deve ter decidido qual serviço de nomes usar para mapeamento de host em seu ambiente.

Passos

1. Adicione as entradas necessárias à tabela do switch de serviço de nomes:

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Verifique se a tabela do switch de serviço de nomes contém as entradas esperadas na ordem desejada:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Exemplo

O exemplo a seguir modifica uma entrada na tabela de switch de serviço de nomes para SVM VS1 para primeiro usar o arquivo hosts locais e, em seguida, um servidor DNS externo para resolver nomes de host:

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

Gerenciar a tabela hosts (somente administradores de cluster)

Um administrador de cluster pode adicionar, modificar, excluir e exibir as entradas de nome de host na tabela hosts da máquina virtual de armazenamento de administrador (SVM). Um administrador do SVM pode configurar as entradas de nome de host

somente para o SVM atribuído.

Comandos para gerenciar entradas locais de nome de host

Você pode usar o `vserver services name-service dns hosts` comando para criar, modificar ou excluir entradas de tabela de host DNS.

Ao criar ou modificar as entradas de nome de host DNS, você pode especificar vários endereços de alias separados por vírgulas.

Se você quiser…	Use este comando…
Crie uma entrada de nome de host DNS	`vserver services name-service dns hosts create`
Modificar uma entrada de nome de host DNS	`vserver services name-service dns hosts modify`
Excluir uma entrada de nome de host DNS	`vserver services name-service dns hosts delete`

Para obter mais informações sobre os `vserver services name-service dns hosts` comandos, consulte "Referência do comando ONTAP" .

Proteja a sua rede

Configurar a segurança da rede usando padrões federais de processamento de informações (FIPS)

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode ativar e desativar o modo SSL FIPS, definir protocolos SSL globalmente e desativar quaisquer cifras fracas, como RC4 dentro do ONTAP.

Por padrão, o SSL no ONTAP é definido com conformidade FIPS desativada e o protocolo SSL habilitado com o seguinte:

- TLSv1,3 (começando em ONTAP 9.11,1)
- TLSv1.2
- TLSv1.1
- TLSv1

Quando o modo SSL FIPS está ativado, a comunicação SSL do ONTAP para clientes externos ou componentes de servidor fora do ONTAP usará criptografia compatível com FIPS para SSL.

Se você quiser que as contas de administrador acessem SVMs com uma chave pública SSH, certifique-se de que o algoritmo da chave do host seja suportado antes de ativar o modo SSL FIPS.

Nota: o suporte ao algoritmo da chave do host foi alterado no ONTAP 9.11,1 e versões posteriores.

Lançamento do ONTAP	Tipos de chave suportados	Tipos de chave não suportados
9.11.1 e mais tarde	ecdsa-sha2-nistp256	rsa-sha2-512 mais rsa-sha2-256 mais ssh-ed25519 mais ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ssh-dss e ssh-rsa

Contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado antes de ativar o FIPS, ou a autenticação do administrador falhará.

Para obter mais informações, "Ativar contas de chave pública SSH"consulte .

Para obter mais informações sobre a configuração do modo SSL FIPS, consulte a `security config modify` página de manual.

Ativar FIPS

É recomendável que todos os usuários seguros ajustem sua configuração de segurança imediatamente após a instalação ou atualização do sistema. Quando o modo SSL FIPS está ativado, a comunicação SSL do ONTAP para clientes externos ou componentes de servidor fora do ONTAP usará criptografia compatível com FIPS para SSL.

> Quando o FIPS está ativado, não é possível instalar ou criar um certificado com um comprimento de chave RSA de 4096.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ativar FIPS:

   ```
   security config modify -interface SSL -is-fips-enabled true
   ```

3. Quando solicitado a continuar, digite `y`
4. Se você estiver executando o ONTAP 9.8 ou anterior reinicialize manualmente cada nó no cluster um por um. A partir do ONTAP 9.9,1, a reinicialização não é necessária.

Exemplo

Se estiver a executar o ONTAP 9.9,1 ou posterior, não verá a mensagem de aviso.

```
security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Desativar FIPS

Se você ainda estiver executando uma configuração de sistema mais antiga e quiser configurar o ONTAP com compatibilidade com versões anteriores, você poderá ativar o SSLv3 somente quando o FIPS estiver desativado.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Desative o FIPS digitando:

   ```
   security config modify -interface SSL -is-fips-enabled false
   ```

3. Quando solicitado a continuar, digite `y`.
4. Se você estiver executando o ONTAP 9.8 ou anterior, reinicie manualmente cada nó no cluster. A partir do ONTAP 9.9,1, a reinicialização não é necessária.

Exemplo

Se estiver a executar o ONTAP 9.9,1 ou posterior, não verá a mensagem de aviso.

```
security config modify -interface SSL -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Visualizar o status de conformidade FIPS

Você pode ver se todo o cluster está executando as configurações de segurança atuais.

Passos

1. Um por um, reinicie cada nó no cluster.

   Não reinicie todos os nós de cluster simultaneamente. É necessário reinicializar para garantir que todos os aplicativos do cluster estejam executando a nova configuração de segurança e todas as alterações no modo de ativação/desativação FIPS, protocolos e cifras.

2. Exibir o status de conformidade atual:

   ```
   security config show
   ```

```
security config show

          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                             !EXP:!eNULL
```

Configurar a criptografia IPsec em trânsito

Prepare-se para usar a segurança IP

A partir do ONTAP 9.8, você tem a opção de usar a segurança IP (IPsec) para proteger o tráfego de rede. IPsec é uma das várias opções de criptografia de dados em movimento

ou em trânsito disponíveis com o ONTAP. Você deve se preparar para configurar o IPsec antes de usá-lo em um ambiente de produção.

Implementação de segurança IP no ONTAP

IPsec é um padrão de Internet mantido pelo IETF. Ele fornece criptografia e integridade de dados, bem como autenticação para o tráfego que flui entre os endpoints da rede em um nível IP.

Com o ONTAP, o IPsec protege todo o tráfego IP entre o ONTAP e os vários clientes, incluindo os protocolos NFS, SMB e iSCSI. Além da privacidade e integridade dos dados, o tráfego de rede é protegido contra vários ataques, como repetição e ataques man-in-the-middle. O ONTAP usa a implementação do modo de transporte IPsec. Ele aproveita o protocolo IKE (Internet Key Exchange) versão 2 para negociar o material chave entre o ONTAP e os clientes usando IPv4 ou IPv6.

Quando o recurso IPsec está ativado em um cluster, a rede requer uma ou mais entradas no banco de dados de diretiva de segurança (SPD) do ONTAP que correspondam às várias caraterísticas de tráfego. Essas entradas mapeiam para os detalhes de proteção específicos necessários para processar e enviar os dados (como, por exemplo, conjunto de codificações e método de autenticação). Uma entrada SPD correspondente também é necessária em cada cliente.

Para certos tipos de tráfego, outra opção de criptografia de dados em movimento pode ser preferível. Por exemplo, para a criptografia do tráfego de peering de cluster e NetApp SnapMirror, o protocolo TLS (Transport Layer Security) geralmente é recomendado em vez de IPsec. Isso ocorre porque o TLS oferece melhor desempenho na maioria das situações.

Informações relacionadas

- "Internet Engineering Task Force"
- "RFC 4301: Arquitetura de segurança para o Protocolo de Internet"

Evolução da implementação IPsec do ONTAP

O IPsec foi introduzido pela primeira vez com o ONTAP 9.8. A implementação continuou a evoluir e melhorar, conforme descrito abaixo.

> Quando um recurso é introduzido a partir de uma versão específica do ONTAP, ele também é suportado em versões subsequentes, a menos que indicado de outra forma.

ONTAP 9.16,1

Várias operações criptográficas, como verificações de criptografia e integridade, podem ser descarregadas para uma placa NIC suportada. Consulte Recurso de descarga de hardware IPsec para obter mais informações.

ONTAP 9.12,1

O suporte ao protocolo de host front-end IPsec está disponível nas configurações de conexão de malha MetroCluster IP e MetroCluster. O suporte IPsec fornecido com clusters MetroCluster é limitado ao tráfego de host front-end e não é compatível com LIFs MetroCluster entre clusters.

ONTAP 9.10,1

Os certificados podem ser usados para autenticação IPsec, além das chaves pré-compartilhadas (PSKs). Antes do ONTAP 9.10,1, apenas PSKs são suportados para autenticação.

ONTAP 9.9,1

Os algoritmos de criptografia usados pelo IPsec são validados pelo FIPS 140-2. Esses algoritmos são

processados pelo módulo criptográfico NetApp no ONTAP, que carrega a validação FIPS 140-2.

ONTAP 9,8

O suporte para IPsec torna-se inicialmente disponível com base na implementação do modo de transporte.

Recurso de descarga de hardware IPsec

Se você estiver usando o ONTAP 9.16,1 ou posterior, terá a opção de descarregar determinadas operações computacionalmente intensivas, como verificações de criptografia e integridade, para uma placa de controlador de interface de rede (NIC) instalada no nó de armazenamento. O uso dessa opção de descarga de hardware pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido por IPsec.

Requisitos e recomendações

Há vários requisitos que você deve considerar antes de usar o recurso de descarga de hardware IPsec.

Placas Ethernet suportadas

Você precisa instalar e usar apenas placas Ethernet compatíveis nos nós de storage. As seguintes placas Ethernet são suportadas com o ONTAP 9.16,1:

- X50131A (controlador Ethernet 2P, 40G/100g/200g/400G CX7)
- X60243A (4P, controlador Ethernet 10G/25G CX7)

Escopo do cluster

O recurso de descarga de hardware IPsec é configurado globalmente para o cluster. E assim, por exemplo, o comando `security ipsec config` se aplica a todos os nós no cluster.

Configuração consistente

As placas NIC suportadas devem ser instaladas em todos os nós do cluster. Se uma placa NIC suportada estiver disponível apenas em alguns dos nós, você poderá ver uma degradação significativa do desempenho após um failover se algumas LIFs não estiverem hospedadas em uma NIC compatível com descarga.

Desativar a anti-repetição

Você deve desativar a proteção anti-replay IPsec no ONTAP (configuração padrão) e nos clientes IPsec. Se não estiver desativado, a fragmentação e o multi-path (rota redundante) não serão suportados.

Limitações

Há várias limitações que você deve considerar antes de usar o recurso de descarga de hardware IPsec.

IPv6

A versão 6 do IP não é suportada para o recurso de descarga de hardware IPsec. O IPv6 só é suportado com a implementação do software IPsec.

Números de sequência alargados

Os números de sequência estendida IPsec não são suportados com o recurso de descarga de hardware. Apenas são utilizados os números normais de sequência de 32 bits.

Agregação de links

O recurso de descarga de hardware IPsec não suporta agregação de links. E assim não pode ser usado com uma interface ou grupo de agregação de links conforme administrado através dos `network port ifgrp` comandos na CLI do ONTAP.

Suporte à configuração na CLI do ONTAP

Três comandos CLI existentes são atualizados no ONTAP 9.16,1 para suportar o recurso de descarga de hardware IPsec, conforme descrito abaixo. Consulte também "Configure a segurança IP no ONTAP"para obter mais informações.

Comando ONTAP	Atualização
`security ipsec config show`	O parâmetro booleano `Offload Enabled` mostra o status atual de descarga da NIC.
`security ipsec config modify`	O parâmetro `is-offload-enabled` pode ser usado para ativar ou desativar o recurso de descarga de NIC.
`security ipsec config show-ipsecsa`	Quatro novos contadores foram adicionados para exibir o tráfego de entrada, bem como de saída em bytes e pacotes.

Suporte à configuração na API REST do ONTAP

Dois endpoints de API REST existentes são atualizados no ONTAP 9.16,1 para oferecer suporte ao recurso de descarga de hardware IPsec, conforme descrito abaixo.

Endpoint da REST	Atualização
`/api/security/ipsec`	O parâmetro `offload_enabled` foi adicionado e está disponível com o método DE PATCH.
`/api/security/ipsec/security_association`	Dois novos valores de contador foram adicionados para rastrear o total de bytes e pacotes processados pelo recurso de descarga.

Saiba mais sobre a API REST do ONTAP, incluindo "Novidades com a API REST do ONTAP", na documentação de automação do ONTAP. Você também deve consultar a documentação de automação do ONTAP para obter detalhes sobre "Pontos de extremidade IPsec"o .

Configure a segurança IP no ONTAP

Há várias tarefas que você precisa executar para configurar e ativar a criptografia IPsec em trânsito no cluster do ONTAP.

> Certifique-se de revisar "Prepare-se para usar a segurança IP" antes de configurar o IPsec. Por exemplo, talvez seja necessário decidir se deve usar o recurso de descarga de hardware IPsec disponível a partir do ONTAP 9.16,1.

Ative o IPsec no cluster

Você pode habilitar o IPsec no cluster para garantir que os dados estejam criptografados continuamente e seguros enquanto estiverem em trânsito.

Passos

1. Descubra se o IPsec já está habilitado:

```
security ipsec config show
```

Se o resultado incluir `IPsec Enabled: false`, avance para o passo seguinte.

2. Ativar IPsec:

   ```
   security ipsec config modify -is-enabled true
   ```

   Você pode ativar o recurso de descarga de hardware IPsec usando o parâmetro booleano `is-offload-enabled`.

3. Execute o comando Discovery novamente:

   ```
   security ipsec config show
   ```

   O resultado agora `IPsec Enabled: true`inclui .

Prepare-se para a criação de diretiva IPsec com autenticação de certificado

Você pode ignorar esta etapa se estiver usando apenas chaves pré-compartilhadas (PSKs) para autenticação e não usar autenticação de certificado.

Antes de criar uma diretiva IPsec que usa certificados para autenticação, você deve verificar se os seguintes pré-requisitos são atendidos:

- Tanto o ONTAP quanto o cliente devem ter o certificado CA da outra parte instalado para que os certificados da entidade final (ONTAP ou cliente) sejam verificáveis por ambos os lados
- Um certificado é instalado para o ONTAP LIF que participa da política

ONTAP LIFs podem compartilhar certificados. Não é necessário um mapeamento individual entre certificados e LIFs.

Passos

1. Instale todos os certificados de CA usados durante a autenticação mútua, incluindo CAs do lado do ONTAP e do lado do cliente, no gerenciamento de certificados do ONTAP, a menos que ele já esteja instalado (como é o caso de uma CA raiz autoassinada do ONTAP).
   - Exemplo de comando*
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. Para garantir que a CA instalada esteja dentro do caminho de pesquisa da CA IPsec durante a autenticação, adicione as CAs de gerenciamento de certificados ONTAP ao módulo IPsec usando o `security ipsec ca-certificate add` comando.
   - Exemplo de comando*
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. Crie e instale um certificado para uso pelo ONTAP LIF. A CA do emissor deste certificado já deve ser instalada no ONTAP e adicionada ao IPsec.
   - Exemplo de comando*
     ```
     cluster::> security certificate install -vserver svm_name -type server -cert
     -name my_nfs_server_cert
     ```

Para obter mais informações sobre certificados no ONTAP, consulte os comandos do certificado de segurança

na documentação do ONTAP 9.

Definir o banco de dados de políticas de segurança (SPD)

O IPsec requer uma entrada SPD antes de permitir que o tráfego flua na rede. Isso é verdade se você estiver usando um PSK ou um certificado para autenticação.

Passos

1. Use o `security ipsec policy create` comando para:
   a. Selecione o endereço IP do ONTAP ou a sub-rede de endereços IP para participar do transporte IPsec.
   b. Selecione os endereços IP do cliente que se conetarão aos endereços IP do ONTAP.

      O cliente deve suportar o Internet Key Exchange versão 2 (IKEv2) com uma chave pré-compartilhada (PSK).

   c. Opcional. Selecione os parâmetros de tráfego detalhados, como os protocolos da camada superior (UDP, TCP, ICMP, etc.), os números de porta local e os números de porta remota para proteger o tráfego. Os parâmetros correspondentes são `protocols`, `local-ports` e `remote-ports` respetivamente.

      Ignore esta etapa para proteger todo o tráfego entre o endereço IP do ONTAP e o endereço IP do cliente. Proteger todo o tráfego é o padrão.

   d. Insira PSK ou infra-estrutura de chave pública (PKI) para `auth-method` o parâmetro para o método de autenticação desejado.
      i. Se você inserir um PSK, inclua os parâmetros e pressione <enter> para que o prompt digite e verifique a chave pré-compartilhada.

         Os `local-identity` parâmetros e `remote-identity` são opcionais se o host e o cliente usarem strongSwan e nenhuma política de curinga for selecionada para o host ou cliente.

      ii. Se introduzir uma PKI, terá de introduzir também os `cert-name` `local-identity` parâmetros , . `remote-identity` Se a identidade do certificado do lado remoto for desconhecida ou se forem esperadas várias identidades de cliente, insira a identidade `ANYTHING`especial .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

O tráfego IP não pode fluir entre o cliente e o servidor até que o ONTAP e o cliente tenham configurado as

diretivas IPsec correspondentes e as credenciais de autenticação (PSK ou certificado) estejam no lugar em ambos os lados.

Use identidades IPsec

Para o método de autenticação de chave pré-compartilhada, identidades locais e remotas são opcionais se o host e o cliente usarem strongSwan e nenhuma política de curinga for selecionada para o host ou cliente.

Para o método de autenticação PKI/certificado, as identidades locais e remotas são obrigatórias. As identidades especificam qual identidade é certificada no certificado de cada lado e são usadas no processo de verificação. Se a identidade remota for desconhecida ou se puder ser muitas identidades diferentes, use a identidade `ANYTHING`especial .

Sobre esta tarefa

Dentro do ONTAP, as identidades são especificadas modificando a entrada SPD ou durante a criação da política SPD. O SPD pode ser um endereço IP ou um nome de identidade de formato de cadeia de carateres.

Passos

1. Use o seguinte comando para modificar uma configuração de identidade SPD existente:

```
security ipsec policy modify
```

Exemplo de comando

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

Configuração de vários clientes IPsec

Quando um pequeno número de clientes precisa aproveitar o IPsec, usar uma única entrada SPD para cada cliente é suficiente. No entanto, quando centenas ou mesmo milhares de clientes precisam utilizar o IPsec, o NetApp recomenda o uso de uma configuração de vários clientes IPsec.

Sobre esta tarefa

O ONTAP é compatível com a conexão de vários clientes em várias redes a um único endereço IP SVM com IPsec ativado. Você pode fazer isso usando um dos seguintes métodos:

- **Configuração de sub-rede**

  Para permitir que todos os clientes em uma sub-rede específica (por exemplo, 192.168.134.0/24) se conetem a um único endereço IP SVM usando uma única entrada de política SPD, você deve especificar o `remote-ip-subnets` formulário de sub-rede in. Além disso, você deve especificar o `remote-identity` campo com a identidade do lado do cliente correta.

  > Ao usar uma única entrada de diretiva em uma configuração de sub-rede, os clientes IPsec nessa sub-rede compartilham a identidade IPsec e a chave pré-compartilhada (PSK). No entanto, isso não é verdade com a autenticação de certificado. Ao usar certificados, cada cliente pode usar seu próprio certificado exclusivo ou um certificado compartilhado para autenticar. O IPsec do ONTAP verifica a validade do certificado com base nas CAs instaladas em seu armazenamento de confiança local. O ONTAP também suporta verificação de lista de revogação de certificados (CRL).

- **Permitir a configuração de todos os clientes**

Para permitir que qualquer cliente, independentemente do endereço IP de origem, se conete ao endereço IP habilitado para IPsec SVM, use o `0.0.0.0/0` caractere curinga ao especificar o `remote-ip-subnets` campo.

Além disso, você deve especificar o `remote-identity` campo com a identidade do lado do cliente correta. Para autenticação de certificado, pode introduzir `ANYTHING`.

Além disso, quando o `0.0.0.0/0` caractere curinga é usado, você deve configurar um número de porta local ou remota específico para usar. Por exemplo, `NFS port 2049`.

Passos

a. Use um dos comandos a seguir para configurar o IPsec para vários clientes.

   i. Se você estiver usando **configuração de sub-rede** para oferecer suporte a vários clientes IPsec:

   ```
   security ipsec policy create -vserver vserver_name -name policy_name
   -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
   IP_address/subnet -local-identity local_id -remote-identity remote_id
   ```

Exemplo de comando

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

   i. Se você estiver usando **permitir que a configuração de todos os clientes** ofereça suporte a vários clientes IPsec:

   ```
   security ipsec policy create -vserver vserver_name -name policy_name
   -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
   -ports port_number -local-identity local_id -remote-identity remote_id
   ```

Exemplo de comando

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Exibir estatísticas IPsec

Por meio da negociação, um canal de segurança chamado Associação de Segurança IKE (SA) pode ser estabelecido entre o endereço IP do ONTAP SVM e o endereço IP do cliente. As SAS IPsec são instaladas em ambos os endpoints para fazer o trabalho real de criptografia e descriptografia de dados. Você pode usar comandos de estatísticas para verificar o status de SAS IPsec e SAS IKE.

> Se você estiver usando o recurso de descarga de hardware IPsec, vários novos contadores serão exibidos com o comando `security ipsec config show-ipsecsa`.

Comandos de exemplo

Comando de exemplo IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Comando e saída de amostra IPsec SA:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Comando e saída de amostra IPsec SA:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Configurar políticas de firewall para LIFs

A configuração de um firewall aumenta a segurança do cluster e ajuda a impedir o acesso não autorizado ao sistema de armazenamento. Por padrão, o firewall integrado é configurado para permitir acesso remoto a um conjunto específico de serviços IP para dados, gerenciamento e LIFs entre clusters.

Começando com ONTAP 9.10,1:

- As políticas de firewall são obsoletas e são substituídas por políticas de serviço LIF. Anteriormente, o firewall integrado era gerenciado usando políticas de firewall. Essa funcionalidade agora é realizada usando uma política de serviço LIF.
- Todas as políticas de firewall estão vazias e não abrem nenhuma porta no firewall subjacente. Em vez disso, todas as portas devem ser abertas usando uma política de serviço LIF.
- Nenhuma ação é necessária após uma atualização para 9.10.1 ou posterior para a transição de políticas de firewall para políticas de serviço LIF. O sistema constrói automaticamente políticas de serviço LIF consistentes com as políticas de firewall em uso na versão anterior do ONTAP. Se você usar scripts ou outras ferramentas que criam e gerenciam políticas de firewall personalizadas, talvez seja necessário atualizar esses scripts para criar políticas de serviço personalizadas.

Para saber mais, "LIFs e políticas de serviço no ONTAP 9.6 e posteriores"consulte .

As políticas de firewall podem ser usadas para controlar o acesso a protocolos de serviço de gerenciamento, como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS ou SNMP. Não é possível definir políticas de firewall para protocolos de dados como NFS ou SMB.

Você pode gerenciar o serviço de firewall e as políticas das seguintes maneiras:

- Ativar ou desativar o serviço de firewall
- Exibindo a configuração atual do serviço de firewall
- Criar uma nova política de firewall com o nome da política e os serviços de rede especificados
- Aplicar uma política de firewall a uma interface lógica
- Criar uma nova política de firewall que seja uma cópia exata de uma política existente

  Use isso para criar uma política com características semelhantes no mesmo SVM ou para copiar a política para um SVM diferente.

- Exibindo informações sobre políticas de firewall
- Modificar os endereços IP e as máscaras de rede que são usadas por uma política de firewall
- Eliminar uma política de firewall que não está a ser utilizada por um LIF

Políticas de firewall e LIFs

As políticas de firewall LIF são usadas para restringir o acesso ao cluster em cada LIF. Você precisa entender como a política de firewall padrão afeta o acesso do sistema sobre cada tipo de LIF e como você pode personalizar uma política de firewall para aumentar ou diminuir a segurança sobre um LIF.

Ao configurar um LIF usando o `network interface create` comando ou `network interface modify`, o valor especificado para o `-firewall-policy` parâmetro determina os protocolos de serviço e os endereços IP que têm acesso permitido ao LIF.

Em muitos casos, você pode aceitar o valor padrão da política de firewall. Em outros casos, talvez seja necessário restringir o acesso a determinados endereços IP e a determinados protocolos de serviço de gerenciamento. Os protocolos de serviço de gerenciamento disponíveis incluem SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS e SNMP.

A política de firewall para todas as LIFs de cluster é padrão `""` e não pode ser modificada.

A tabela a seguir descreve as políticas de firewall padrão que são atribuídas a cada LIF, dependendo de sua função (ONTAP 9.5 e anterior) ou diretiva de serviço (ONTAP 9.6 e posterior), quando você cria o LIF:

Política de firewall	Protocolos de serviço padrão	Acesso predefinido	LIFs aplicadas a
gestão	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualquer endereço (0,0.0,0/0)	Gerenciamento de clusters, gerenciamento de SVM e LIFs de gerenciamento de nós

gerenciamento nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualquer endereço (0,0.0,0/0)	LIFs de dados que também são compatíveis com o acesso de gerenciamento da SVM
entre clusters	https, ndmp, ndmps	Qualquer endereço (0,0.0,0/0)	Todos os LIFs entre clusters
dados	dns, ndmp, ndmps, portmap	Qualquer endereço (0,0.0,0/0)	Todos os dados LIFs

Configuração do serviço portmap

O serviço portmap mapeia os serviços RPC para as portas nas quais eles escutam.

O serviço portmap estava sempre acessível no ONTAP 9.3 e anterior, tornou-se configurável no ONTAP 9.4 através do ONTAP 9.6 e é gerenciado automaticamente a partir do ONTAP 9.7.

- No ONTAP 9.3 e anteriores, o serviço portmap (rpcbind) estava sempre acessível na porta 111 em configurações de rede que dependiam do firewall ONTAP integrado em vez de um firewall de terceiros.
- Do ONTAP 9.4 ao ONTAP 9.6, você pode modificar políticas de firewall para controlar se o serviço portmap está acessível em LIFs específicos.
- A partir do ONTAP 9.7, o serviço de firewall portmap é eliminado. Em vez disso, a porta portmap é aberta automaticamente para todos os LIFs que suportam o serviço NFS.

O serviço portmap é configurável no firewall no ONTAP 9.4 através do ONTAP 9.6.

O restante deste tópico discute como configurar o serviço de firewall do portmap para as versões do ONTAP 9.4 através do ONTAP 9.6.

Dependendo da sua configuração, você poderá desativar o acesso ao serviço em tipos específicos de LIFs, geralmente de gerenciamento e LIFs entre clusters. Em algumas circunstâncias, você pode até mesmo ser capaz de proibir o acesso em LIFs de dados.

Que comportamento você pode esperar

O comportamento do ONTAP 9.4 até o ONTAP 9.6 foi projetado para fornecer uma transição perfeita na atualização. Se o serviço portmap já estiver sendo acessado sobre tipos específicos de LIFs, ele continuará acessível sobre esses tipos de LIFs. Como no ONTAP 9.3 e anteriores, você pode especificar os serviços acessíveis no firewall na política de firewall para o tipo LIF.

Todos os nós no cluster devem estar executando o ONTAP 9.4 a ONTAP 9.6 para que o comportamento entre em vigor. Apenas o tráfego de entrada é afetado.

As novas regras são as seguintes:

- Ao atualizar para a versão 9,4 até 9,6, o ONTAP adiciona o serviço portmap a todas as políticas de firewall existentes, padrão ou personalizado.
- Quando você cria um novo cluster ou um novo espaço de IPspace, o ONTAP adiciona o serviço de portmap apenas à política de dados padrão, não ao gerenciamento padrão ou às políticas entre clusters.
- Você pode adicionar o serviço portmap a políticas padrão ou personalizadas conforme necessário e remover o serviço conforme necessário.

Como adicionar ou remover o serviço portmap

Para adicionar o serviço portmap a uma diretiva de firewall de cluster ou SVM (torná-lo acessível dentro do firewall), digite:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Para remover o serviço portmap de uma diretiva de firewall de cluster ou SVM (torná-lo inacessível no firewall), digite:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Você pode usar o comando Network Interface Modify para aplicar a política de firewall a um LIF existente. Para obter a sintaxe de comando completa, consulte "Referência do comando ONTAP" .

Crie uma política de firewall e atribua-a a um LIF

As políticas de firewall padrão são atribuídas a cada LIF quando você cria o LIF. Em muitos casos, as configurações padrão do firewall funcionam bem e você não precisa alterá-las. Se você quiser alterar os serviços de rede ou endereços IP que podem acessar um LIF, você pode criar uma política de firewall personalizada e atribuí-la ao LIF.

Sobre esta tarefa

- Não é possível criar uma política de firewall com o `policy` nome `data`, `intercluster`, `cluster`, ou `mgmt`.

  Esses valores são reservados para as políticas de firewall definidas pelo sistema.

- Não é possível definir ou modificar uma política de firewall para LIFs de cluster.

  A política de firewall para LIFs de cluster está definida como 0,0.0.0/0 para todos os tipos de serviços.

- Se você precisar remover um serviço de uma política, exclua a política de firewall existente e crie uma nova política.
- Se o IPv6 estiver ativado no cluster, você poderá criar políticas de firewall com endereços IPv6.

  Depois que o IPv6 estiver ativado, `data` `intercluster`, e `mgmt` as políticas de firewall incluem ::/0, o curinga IPv6, em sua lista de endereços aceitos.

- Ao usar o System Manager para configurar a funcionalidade de proteção de dados entre clusters, você deve garantir que os endereços IP LIF sejam incluídos na lista permitida e que o serviço HTTPS seja permitido tanto nas LIFs entre clusters quanto nas firewalls de propriedade da empresa.

  Por padrão, a `intercluster` política de firewall permite o acesso de todos os endereços IP (0,0.0,0/0, ou ::/0 para IPv6) e habilita os serviços HTTPS, NDMP e NDMPS. Se você modificar essa política padrão ou criar sua própria política de firewall para LIFs entre clusters, adicione cada endereço IP LIF entre clusters à lista permitida e ative o serviço HTTPS.

- A partir do ONTAP 9.6, os serviços de firewall HTTPS e SSH não são suportados.

  No ONTAP 9.6, os `management-https` serviços e `management-ssh` LIF estão disponíveis para acesso de gerenciamento HTTPS e SSH.

Passos

1. Crie uma política de firewall que estará disponível para os LIFs em um SVM específico:

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   Você pode usar este comando várias vezes para adicionar mais de um serviço de rede e lista de endereços IP permitidos para cada serviço na política de firewall.

2. Verifique se a política foi adicionada corretamente usando o `system services firewall policy show` comando.
3. Aplique a política de firewall a um LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Verifique se a política foi adicionada corretamente ao LIF usando o `network interface show -fields firewall-policy` comando.

Exemplo de criar uma política de firewall e atribuí-la a um LIF

O comando a seguir cria uma política de firewall chamada data_http que habilita o acesso de protocolos HTTP e HTTPS a partir de endereços IP na sub-rede 10,10, aplica essa política ao LIF chamado data1 na SVM VS1 e, em seguida, mostra todas as políticas de firewall no cluster:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

Comandos para gerenciar o serviço e as políticas de firewall

Você pode usar os `system services firewall` comandos para gerenciar o serviço de firewall, os `system services firewall policy` comandos para gerenciar políticas de firewall e o `network interface modify` comando para gerenciar configurações de firewall para LIFs.

Se você quiser…	Use este comando…
Ativar ou desativar o serviço de firewall	`system services firewall modify`
Exibir a configuração atual do serviço de firewall	`system services firewall show`
Crie uma política de firewall ou adicione um serviço a uma política de firewall existente	`system services firewall policy create`
Aplique uma política de firewall a um LIF	`network interface modify -lif lifname -firewall-policy`
Modifique os endereços IP e as máscaras de rede associadas a uma política de firewall	`system services firewall policy modify`
Exibir informações sobre políticas de firewall	`system services firewall policy show`
Crie uma nova política de firewall que seja uma cópia exata de uma política existente	`system services firewall policy clone`
Exclua uma política de firewall que não seja usada por um LIF	`system services firewall policy delete`

Para obter mais informações, consulte as páginas de manual dos `system services firewall` comandos , `system services firewall policy` e `network interface modify`"A referência do comando ONTAP 9" em .

Marcação de QoS (apenas administradores de cluster)

Visão geral do QoS

A marcação de qualidade de serviço (QoS) da rede ajuda a priorizar diferentes tipos de tráfego com base nas condições da rede para utilizar efetivamente os recursos da rede. Você pode definir o valor de ponto de código de serviços diferenciados (DSCP) dos pacotes IP de saída para os tipos de tráfego suportados por espaço de IPspace.

Marcação DSCP para conformidade com UC

Você pode ativar a marcação DSCP (Differentiated Services Code Point) no tráfego de pacotes IP de saída (saída) para um determinado protocolo com um código DSCP padrão ou fornecido pelo usuário. A marcação

DSCP é um mecanismo para classificar e gerenciar o tráfego de rede e é um componente da conformidade com a capacidade Unificada (UC).

A marcação DSCP (também conhecida como *marcação QoS* ou *marcação de qualidade de serviço*) é ativada fornecendo um valor IPspace, protocolo e DSCP. Os protocolos nos quais a marcação DSCP pode ser aplicada são NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet e SNMP.

Se você não fornecer um valor DSCP ao ativar a marcação DSCP para um determinado protocolo, um padrão será usado:

- O valor predefinido para protocolos/tráfego de dados é 0x0A (10).
- O valor predefinido para protocolos de controlo/tráfego é 0x30 (48).

Modificar valores de marcação QoS

Você pode modificar os valores de marcação de qualidade do serviço (QoS) para diferentes protocolos, para cada IPspace.

Antes de começar

Todos os nós no cluster devem estar executando a mesma versão do ONTAP.

Passo

Modifique os valores de marcação de QoS usando o `network qos-marking modify` comando.

- O `-ipspace` parâmetro especifica o espaço IPspace para o qual a entrada de marcação QoS deve ser modificada.
- O `-protocol` parâmetro especifica o protocolo para o qual a entrada de marcação QoS deve ser modificada. A `network qos-marking modify` página man descreve os possíveis valores do protocolo.
- O `-dscp` parâmetro especifica o valor DSCP (Differentiated Services Code Point). Os valores possíveis variam de 0 a 63.
- O `-is-enabled` parâmetro é utilizado para ativar ou desativar a marcação QoS para o protocolo especificado no espaço IPspace fornecido pelo `-ipspace` parâmetro.

O comando a seguir habilita a marcação QoS para o protocolo NFS no IPspace padrão:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

O comando a seguir define o valor DSCP como 20 para o protocolo NFS no IPspace padrão:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Exibir valores de marcação de QoS

Você pode exibir os valores de marcação de QoS para diferentes protocolos, para cada espaço IPspace.

Passo

Exiba valores de marcação de QoS usando o `network qos-marking show` comando.

O comando a seguir exibe a marcação QoS para todos os protocolos no espaço IPspace padrão:

```
network qos-marking show -ipspace Default
IPspace              Protocol           DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                 10  false
                     FTP                  48  false
                     HTTP-admin           48  false
                     HTTP-filesrv         10  false
                     NDMP                 10  false
                     NFS                  10  true
                     SNMP                 48  false
                     SSH                  48  false
                     SnapMirror           10  false
                     Telnet               48  false
                     iSCSI                10  false
11 entries were displayed.
```

Gerenciar SNMP (somente administradores de cluster)

Visão geral da SNMP

Você pode configurar o SNMP para monitorar SVMs em seu cluster para evitar problemas antes que eles ocorram e responder a problemas se eles ocorrerem. O gerenciamento do SNMP envolve a configuração de usuários SNMP e a configuração de destinos de host SNMP (estações de trabalho de gerenciamento) para todos os eventos SNMP. O SNMP está desativado por padrão em LIFs de dados.

Você pode criar e gerenciar usuários SNMP somente leitura no data SVM. As LIFs de dados devem ser configuradas para receber solicitações SNMP no SVM.

As estações de trabalho de gerenciamento de rede SNMP, ou gerentes, podem consultar o agente SNMP SVM para obter informações. O agente SNMP reúne informações e as encaminha para os gerentes SNMP. O agente SNMP também gera notificações de intercetação sempre que ocorrem eventos específicos. O agente SNMP no SVM tem Privileges somente leitura; ele não pode ser usado para nenhuma operação definida ou para tomar uma ação corretiva em resposta a uma armadilha. O ONTAP fornece um agente SNMP compatível com as versões v1, v2c e v3 do SNMP. O SNMPv3 oferece segurança avançada usando senhas e criptografia.

Para obter mais informações sobre o suporte SNMP em sistemas ONTAP, "TR-4220: Suporte SNMP no Data ONTAP" consulte .

Visão geral da MIB

Um MIB (Management Information base) é um arquivo de texto que descreve objetos e traps SNMP.

As MIBs descrevem a estrutura dos dados de gerenciamento do sistema de armazenamento e usam um namespace hierárquico contendo identificadores de objeto (OIDs). Cada OID identifica uma variável que pode ser lida usando SNMP.

Como MIBs não são arquivos de configuração e o ONTAP não lê esses arquivos, a funcionalidade SNMP não é afetada por MIBs. O ONTAP fornece o seguinte arquivo MIB:

- Um MIB personalizado NetApp (`netapp.mib`)

O ONTAP suporta MIBs IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), que mostram dados IPv4 e IPv6, são suportados.

O ONTAP também fornece uma breve referência cruzada entre identificadores de objeto (OIDs) e nomes curtos de objetos no `traps.dat` arquivo.

> As versões mais recentes dos arquivos MIBs ONTAP e 'traps.dat' estão disponíveis no site de suporte da NetApp. No entanto, as versões desses arquivos no site de suporte não correspondem necessariamente aos recursos SNMP de sua versão do ONTAP. Esses arquivos são fornecidos para ajudá-lo a avaliar os recursos SNMP na versão mais recente do ONTAP.

Traps SNMP

Os traps SNMP capturam informações de monitoramento do sistema que são enviadas como uma notificação assíncrona do agente SNMP para o gerenciador SNMP.

Existem três tipos de traps SNMP: Padrão, embutido e definido pelo usuário. Os traps definidos pelo usuário não são suportados no ONTAP.

Uma armadilha pode ser usada para verificar periodicamente se há limites operacionais ou falhas que são definidos na MIB. Se um limite for atingido ou uma falha for detetada, o agente SNMP enviará uma mensagem (trap) aos hosts que os alertam sobre o evento.

> ONTAP suporta SNMPv1 armadilhas e, olhando em ONTAP 9.1, SNMPv3 armadilhas. ONTAP não suporta SNMPv2c armadilhas e informa.

Traps SNMP padrão

Esses traps são definidos no RFC 1215. Existem cinco traps SNMP padrão que são suportados pelo ONTAP: Coldstart, warmStart, linkDown, linkup e autenticationFailure.

> A armadilha autenticationFailure é desativada por padrão. Você deve usar o `system snmp authtrap` comando para ativar a armadilha. Para obter mais informações, consulte as páginas de manual: "Referência do comando ONTAP"

Traps SNMP incorporados

Os traps incorporados são predefinidos no ONTAP e são enviados automaticamente para as estações de gerenciamento de rede na lista de traphost se ocorrer um evento. Essas armadilhas, como diskFailedShutdown, cpuTooBusy e volumeNearlyFull, são definidas no MIB personalizado.

Cada armadilha incorporada é identificada por um código de armadilha exclusivo.

Crie uma comunidade SNMP e atribua-a a um LIF

Você pode criar uma comunidade SNMP que atua como um mecanismo de autenticação entre a estação de gerenciamento e a máquina virtual de armazenamento (SVM) ao usar SNMPv1 e SNMPv2c.

Ao criar comunidades SNMP em um SVM de dados, você pode executar comandos como `snmpwalk` e `snmpget` nas LIFs de dados.

Sobre esta tarefa

- Em novas instalações do ONTAP, o SNMPv1 e o SNMPv2c são desativados por padrão.

  SNMPv1 e SNMPv2c são ativados depois de criar uma comunidade SNMP.

- O ONTAP suporta comunidades somente leitura.
- Por padrão, a política de firewall de "dados" atribuída a LIFs de dados tem serviço SNMP definido como `deny`.

  Você deve criar uma nova política de firewall com serviço SNMP definido como `allow` ao criar um usuário SNMP para um SVM de dados.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- Você pode criar comunidades SNMP para usuários SNMPv1 e SNMPv2c para o SVM admin e o SVM de dados.
- Como um SVM não faz parte do padrão SNMP, as consultas sobre LIFs de dados devem incluir o OID raiz do NetApp (1,3.6,1.4,1.789), por exemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Passos

1. Crie uma comunidade SNMP usando o `system snmp community add` comando. O comando a seguir mostra como criar uma comunidade SNMP no cluster SVM admin-1:

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   O comando a seguir mostra como criar uma comunidade SNMP nos dados SVM VS1:

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. Verifique se as comunidades foram criadas usando o comando system snmp Community show.

   O comando a seguir mostra as duas comunidades criadas para SNMPv1 e SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Verifique se o SNMP é permitido como um serviço na política de firewall de "dados" usando o `system services firewall policy show` comando.

   O comando a seguir mostra que o serviço snmp não é permitido na política de firewall "dados" padrão (o serviço snmp é permitido somente na política de firewall "mgmt"):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Crie uma nova política de firewall que permita o acesso usando `snmp` o serviço usando o `system services firewall policy create` comando.

   Os comandos a seguir criam uma nova política de firewall de dados chamada "data1" que permite o. `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Aplique a política de firewall a um LIF de dados usando o comando 'Network Interface Modify' com o parâmetro -firewall-policy.

   O comando a seguir atribui a nova política de firewall "data1" ao LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Configure SNMPv3 usuários em um cluster

O SNMPv3 é um protocolo seguro quando comparado ao SNMPv1 e ao SNMPv2c. Para utilizar o SNMPv3, tem de configurar um utilizador SNMPv3 para executar os utilitários SNMP a partir do gestor SNMP.

Passo

Use o "security login create command" para criar um usuário SNMPv3.

Você é solicitado a fornecer as seguintes informações:

- ID do motor: O valor predefinido e recomendado é ID do motor local
- Protocolo de autenticação
- Palavra-passe de autenticação
- Protocolo de privacidade
- Senha do protocolo de privacidade

Resultado

O utilizador SNMPv3 pode iniciar sessão a partir do gestor SNMP utilizando o nome de utilizador e a palavra-passe e executar os comandos do utilitário SNMP.

SNMPv3 parâmetros de segurança

O SNMPv3 inclui um recurso de autenticação que, quando selecionado, exige que os usuários digitem seus

nomes, um protocolo de autenticação, uma chave de autenticação e seu nível de segurança desejado ao invocar um comando.

A tabela a seguir lista os parâmetros de segurança SNMPv3 :

Parâmetro	Opção de linha de comando	Descrição
EngineID	-E EngineID	ID do motor do agente SNMP. O valor padrão é local EngineID (recomendado).
SecurityName	-U Nome	O nome de utilizador não deve exceder 32 carateres.
AuthProtocol	-A [none	MD5
SHA	SHA-256]	O tipo de autenticação pode ser None, MD5, SHA ou SHA-256.
Authkey	-UMA FRASE-PASSE	Frase-passe com um mínimo de oito carateres.
Segurançanível	-L [authNoPriv	authPriv
noAuthNoPriv]	O nível de segurança pode ser Autenticação, sem Privacidade; Autenticação, Privacidade; ou sem Autenticação, sem Privacidade.	PrivProtocol
aes128	O protocolo de privacidade pode ser nenhum, des ou AES128	PrivPassword

Exemplos para diferentes níveis de segurança

Este exemplo mostra como um usuário SNMPv3 criado com diferentes níveis de segurança pode usar os comandos do lado do cliente SNMP, como `snmpwalk`, para consultar os objetos do cluster.

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

Você deve usar `snmpwalk` 5.3.1 ou posterior quando o protocolo de autenticação for SHA.

Nível de segurança: AuthPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança authPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Modo FIPS

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nível de segurança: AuthNoPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança authNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Modo FIPS

O FIPS não permite que você escolha **nenhum** para o protocolo de privacidade. Como resultado, não é possível configurar um usuário authNoPriv SNMPv3 no modo FIPS.

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nível de segurança: NoAuthNoPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança noAuthNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Modo FIPS

O FIPS não permite que você escolha **nenhum** para o protocolo de privacidade.

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Configure os traphosts para receber notificações SNMP

Você pode configurar o traphost (gerenciador SNMP) para receber notificações (PDUs de intercetação SNMP) quando os traps SNMP são gerados no cluster. Você pode especificar o nome do host ou o endereço IP (IPv4 ou IPv6) do traphost SNMP.

Antes de começar

- Os traps SNMP e SNMP devem estar ativados no cluster.

> As traps SNMP e SNMP estão ativadas por predefinição.

- O DNS deve ser configurado no cluster para resolver os nomes do traphost.
- O IPv6 deve estar ativado no cluster para configurar os traphosts SNMP usando endereços IPv6.
- Para o ONTAP 9.1 e versões posteriores, você deve ter especificado a autenticação de um modelo de segurança baseado no usuário predefinido (USM) e credenciais de privacidade ao criar traphosts.

Passo

Adicionar um traphost SNMP:

```
system snmp traphost add
```

> Os traps só podem ser enviados quando pelo menos uma estação de gerenciamento SNMP é especificada como um traphost.

O comando a seguir adiciona um novo host SNMPv3 chamado yyy.example.com com um usuário USM conhecido:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

O comando a seguir adiciona um traphost usando o endereço IPv6 do host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Teste a polling SNMP

Depois de configurar o SNMP, você deve verificar se você pode poll o cluster.

Sobre esta tarefa

Para fazer polling de um cluster, você precisa usar um comando de terceiros, `snmpwalk` como o .

Passos

1. Envie um comando SNMP para poll o cluster a partir de um cluster diferente.

   Para sistemas que executam o SNMPv1, use o comando CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

   Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

   Para sistemas que executam o SNMPv2c, use o comando CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

   Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Para sistemas que executam o SNMPv3, use o comando CLI `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Comandos para gerenciar SNMP

Você pode usar os `system snmp` comandos para gerenciar SNMP, traps e traphosts. Você pode usar os `security` comandos para gerenciar usuários SNMP por SVM. Você pode usar os `event` comandos para gerenciar eventos relacionados a traps SNMP.

Comandos para configurar o SNMP

Se você quiser…	Use este comando…
Ative o SNMP no cluster	`options -option-name snmp.enable -option-value on` O serviço SNMP tem de ser permitido na política de firewall de gestão (mgmt). Você pode verificar se o SNMP é permitido usando o comando show de política de firewall de serviços do sistema.
Desative o SNMP no cluster	`options -option-name snmp.enable -option-value off`

Comandos para gerenciar usuários SNMP v1, v2c e v3

Se você quiser…	Use este comando…
Configurar utilizadores SNMP	`security login create`

Exibir usuários SNMP	`security snmpusers and security login show -application snmp`
Eliminar utilizadores SNMP	`security login delete`
Modifique o nome da função de controle de acesso de um método de login para usuários SNMP	`security login modify`

Comandos para fornecer informações de Contato e localização

Se você quiser…	Use este comando…
Apresentar ou modificar os detalhes de contacto do cluster	`system snmp contact`
Exiba ou modifique os detalhes de localização do cluster	`system snmp location`

Comandos para gerenciar comunidades SNMP

Se você quiser…	Use este comando…
Adicione uma comunidade somente leitura (ro) para um SVM ou para todos os SVMs no cluster	`system snmp community add`
Exclua uma comunidade ou todas as comunidades	`system snmp community delete`
Exiba a lista de todas as comunidades	`system snmp community show`

Como os SVMs não fazem parte do padrão SNMP, as consultas sobre LIFs de dados devem incluir o OID raiz do NetApp (1,3.6,1.4,1.789), por exemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Comando para exibir valores de opção SNMP

Se você quiser…	Use este comando…
Exiba os valores atuais de todas as opções SNMP, incluindo Contato de cluster, localização de Contato, se o cluster está configurado para enviar traps, a lista de traphosts e lista de comunidades e tipo de controle de acesso	`system snmp show`

Comandos para gerenciar traps e traphosts SNMP

Se você quiser…	Use este comando…

Ativar traps SNMP enviados a partir do cluster	`system snmp init -init 1`
Desative traps SNMP enviados a partir do cluster	`system snmp init -init 0`
Adicione um traphost que receba notificações SNMP para eventos específicos no cluster	`system snmp traphost add`
Excluir um traphost	`system snmp traphost delete`
Exibir a lista de hosts	`system snmp traphost show`

Comandos para gerenciar eventos relacionados a traps SNMP

Se você quiser…	Use este comando…
Exibir os eventos para os quais são gerados traps SNMP (internos)	`event route show` Utilize o `-snmp-support true` parâmetro para visualizar apenas eventos relacionados com SNMP. Use o `instance -messagename <message>` parâmetro para exibir uma descrição detalhada do motivo pelo qual um evento pode ter ocorrido e qualquer ação corretiva. O roteamento de eventos individuais de intercetação SNMP para destinos específicos de traphost não é suportado. Todos os eventos de intercetação SNMP são enviados para todos os destinos de traphost.
Exibir uma lista de Registros de histórico de trap SNMP, que são notificações de eventos que foram enviadas para traps SNMP	`event snmphistory show`
Eliminar um registo de histórico de trap SNMP	`event snmphistory delete`

Para obter mais informações sobre os `system snmp` comandos , `security` e `event` , consulte "Referência do comando ONTAP".

Gerenciar o roteamento em uma SVM

Visão geral do roteamento SVM

A tabela de roteamento de um SVM determina o caminho de rede que o SVM usa para se comunicar com um destino. É importante entender como as tabelas de roteamento funcionam para que você possa evitar problemas de rede antes que eles ocorram.

As regras de roteamento são as seguintes:

- A ONTAP encaminha o tráfego para a rota mais específica disponível.
- O ONTAP roteia o tráfego por uma rota de gateway padrão (com 0 bits de máscara de rede) como último recurso, quando rotas mais específicas não estão disponíveis.

No caso de rotas com o mesmo destino, máscara de rede e métrica, não há garantia de que o sistema usará a mesma rota após uma reinicialização ou após uma atualização. Isso é especialmente um problema se você tiver configurado várias rotas padrão.

É uma prática recomendada configurar uma rota padrão somente para um SVM. Para evitar interrupções, você deve garantir que a rota padrão seja capaz de alcançar qualquer endereço de rede que não seja acessível por uma rota mais específica. Para obter mais informações, consulte o artigo da base de conhecimento "SU134: O acesso à rede pode ser interrompido por uma configuração de roteamento incorreta no cluster ONTAP"

Crie uma rota estática

Você pode criar rotas estáticas em uma máquina virtual de armazenamento (SVM) para controlar como os LIFs usam a rede para tráfego de saída.

Quando você cria uma entrada de rota associada a um SVM, a rota será usada por todos os LIFs que são de propriedade do SVM especificado e que estão na mesma sub-rede que o gateway.

Passo

Use o `network route create` comando para criar uma rota.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

Ativar o roteamento multipath

Se várias rotas tiverem a mesma métrica para um destino, apenas uma das rotas será selecionada para o tráfego de saída. Isso leva a que outras rotas não sejam utilizadas para enviar tráfego de saída. Você pode habilitar o roteamento multipath para o balanceamento de carga em todas as rotas disponíveis proporcionalmente às suas métricas, em vez do roteamento ECMP, que equilibra a carga entre as rotas disponíveis da mesma métrica.

Passos

1. Inicie sessão no nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ativar o roteamento multipath:

   ```
   network options multipath-routing modify -is-enabled true
   ```

   O roteamento multipath está habilitado para todos os nós no cluster.

```
network options multipath-routing modify -is-enabled true
```

Eliminar uma rota estática no ONTAP

Você pode excluir uma rota estática desnecessária de uma máquina virtual de armazenamento (SVM).

Passo

Use o `network route delete` comando para excluir uma rota estática.

Saiba mais sobre o comando link:http://docs.NetApp.com/US-en/ONTAP-cli/network-route-delete.html[`network route` em referência de comando ONTAP.

O exemplo a seguir exclui uma rota estática associada ao SVM vs0 com um gateway de 10.63.0.1 e um endereço IP de destino de 0,0.0,0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

Exibir informações de roteamento

Você pode exibir informações sobre a configuração de roteamento para cada SVM no cluster. Isso pode ajudá-lo a diagnosticar problemas de roteamento envolvendo problemas de conetividade entre aplicativos ou serviços cliente e um LIF em um nó no cluster.

Passos

1. Use o `network route show` comando para exibir rotas dentro de um ou mais SVMs. O exemplo a seguir mostra uma rota configurada no vs0 SVM:

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. Use o `network route show-lifs` comando para exibir a associação de rotas e LIFs em um ou mais SVMs.

   O exemplo a seguir mostra LIFs com rotas pertencentes ao SVM vs0:

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

3. Use o `network route active-entry show` comando para exibir rotas instaladas em um ou mais nós, SVMs, sub-redes ou rotas com destinos especificados.

   O exemplo a seguir mostra todas as rotas instaladas em um SVM específico:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
```

```
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

Remover rotas dinâmicas das tabelas de roteamento

Quando os redirecionamentos ICMP são recebidos para IPv4 e IPv6, as rotas dinâmicas são adicionadas à tabela de roteamento. Por padrão, as rotas dinâmicas são removidas após 300 segundos. Se você quiser manter rotas dinâmicas por um período de tempo diferente, você pode alterar o valor do tempo limite.

Sobre esta tarefa

Você pode definir o valor de tempo limite de 0 a 65.535 segundos. Se você definir o valor como 0, as rotas nunca expiram. A remoção de rotas dinâmicas impede a perda de conetividade causada pela persistência de rotas inválidas.

Passos

1. Apresentar o valor atual do tempo limite.
   - Para IPv4:

     ```
     network tuning icmp show
     ```

   - Para IPv6:

     ```
     network tuning icmp6 show
     ```

2. Modifique o valor de tempo limite.
   - Para IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

- Para IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

3. Verifique se o valor de tempo limite foi modificado corretamente.
   - Para IPv4:

```
network tuning icmp show
```

   - Para IPv6:

```
network tuning icmp6 show
```

Ver informações da rede

Ver descrição geral das informações da rede

Usando a CLI, você pode exibir informações relacionadas a portas, LIFs, rotas, regras de failover, grupos de failover, regras de firewall, DNS, NIS e conexões. A partir do ONTAP 9.8, você também pode baixar os dados exibidos no Gerenciador de sistema sobre sua rede.

Essas informações podem ser úteis em situações como a reconfiguração das configurações de rede ou na solução de problemas do cluster.

Se você for um administrador de cluster, poderá exibir todas as informações de rede disponíveis. Se você for um administrador de SVM, poderá exibir apenas as informações relacionadas aos SVMs atribuídos.

No System Manager, quando você exibe informações em uma *List View*, você pode clicar em **Download** e a lista de objetos exibidos é baixada.

- A lista é baixada no formato CSV (valores separados por vírgula).
- Apenas os dados nas colunas visíveis são transferidos.
- O nome do arquivo CSV é formatado com o nome do objeto e um carimbo de hora.

Exibir informações da porta de rede

Você pode exibir informações sobre uma porta específica ou sobre todas as portas em todos os nós do cluster.

Sobre esta tarefa

São apresentadas as seguintes informações:

- Nome do nó
- Nome da porta
- Nome do IPspace
- Nome de domínio de broadcast
- Estado da ligação (para cima ou para baixo)
- Definição MTU
- Configuração da velocidade da porta e status operacional (1 Gigabit ou 10 gigabits por segundo)
- Configuração de negociação automática (verdadeiro ou falso)
- Modo duplex e estado operacional (meio ou cheio)
- O grupo de interfaces da porta, se aplicável
- As informações da etiqueta VLAN da porta, se aplicável
- Estado de integridade da porta (estado ou degradado)
- Razões para uma porta ser marcada como degradada

Se os dados de um campo não estiverem disponíveis (por exemplo, o duplex operacional e a velocidade de uma porta inativa não estarão disponíveis), o valor do campo será listado como `-`.

Passo

Exiba as informações da porta de rede usando o `network port show` comando.

Você pode exibir informações detalhadas para cada porta especificando o `-instance` parâmetro ou obter informações específicas especificando nomes de campos usando o `-fields` parâmetro.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

Exibir informações sobre uma VLAN (somente administradores de cluster)

Você pode exibir informações sobre uma VLAN específica ou sobre todas as VLANs no cluster.

Sobre esta tarefa

Você pode exibir informações detalhadas para cada VLAN especificando o `-instance` parâmetro. Você pode exibir informações específicas especificando nomes de campos usando o `-fields` parâmetro.

Passo

Exiba informações sobre VLANs usando o `network port vlan show` comando. O comando a seguir exibe informações sobre todas as VLANs no cluster:

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

Exibir informações do grupo de interfaces (somente administradores de cluster)

Você pode exibir informações sobre um grupo de interfaces para determinar sua configuração.

Sobre esta tarefa

São apresentadas as seguintes informações:

- Nó no qual o grupo de interfaces está localizado
- Lista de portas de rede incluídas no grupo de interfaces
- Nome do grupo de interfaces
- Função de distribuição (MAC, IP, porta ou sequencial)
- Endereço MAC (Media Access Control) do grupo de interfaces
- Status da atividade da porta; ou seja, se todas as portas agregadas estão ativas (participação total), se algumas estão ativas (participação parcial) ou se nenhuma está ativa

Passo

Exiba informações sobre grupos de interface usando o `network port ifgrp show` comando.

Você pode exibir informações detalhadas para cada nó especificando o `-instance` parâmetro. Você pode exibir informações específicas especificando nomes de campos usando o `-fields` parâmetro.

O comando a seguir exibe informações sobre todos os grupos de interface no cluster:

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

O comando a seguir exibe informações detalhadas do grupo de interfaces para um único nó:

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

Apresentar informações de LIF

Você pode visualizar informações detalhadas sobre um LIF para determinar sua configuração.

Você também pode querer exibir essas informações para diagnosticar problemas básicos de LIF, como verificar endereços IP duplicados ou verificar se a porta de rede pertence à sub-rede correta. Os administradores de máquina virtual de armazenamento (SVM) podem exibir apenas as informações sobre os LIFs associados ao SVM.

Sobre esta tarefa

São apresentadas as seguintes informações:

- Endereço IP associado ao LIF
- Estado administrativo do LIF
- Status operacional do LIF

  O status operacional das LIFs de dados é determinado pelo status do SVM com o qual as LIFs de dados

estão associadas. Quando o SVM é interrompido, o status operacional do LIF muda para baixo. Quando o SVM é iniciado novamente, o status operacional muda para up

- Nó e a porta na qual reside o LIF

Se os dados de um campo não estiverem disponíveis (por exemplo, se não houver informações de status estendidas), o valor do campo será listado como −.

Passo

Exiba informações de LIF usando o comando network interface show.

Você pode visualizar informações detalhadas para cada LIF especificando o parâmetro -instância ou obter informações específicas especificando nomes de campos usando o parâmetro -fields.

O comando a seguir exibe informações gerais sobre todos os LIFs em um cluster:

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

O comando a seguir mostra informações detalhadas sobre um único LIF:

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
              Operational Status: up
                 Extended Status: -
                         Is Home: false
                 Network Address: 192.0.2.128
                         Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

Exibir informações de roteamento

É possível exibir informações sobre rotas em um SVM.

Passo

Dependendo do tipo de informações de roteamento que você deseja exibir, digite o comando aplicável:

Para ver informações sobre…	Digite…
Rotas estáticas, por SVM	`network route show`
LIFs em cada rota, por SVM	`network route show-lifs`

Você pode exibir informações detalhadas para cada rota especificando o `-instance` parâmetro. O comando a seguir exibe as rotas estáticas dentro dos SVMs no cluster- 1:

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

O comando a seguir exibe a associação de rotas estáticas e interfaces lógicas (LIFs) em todos os SVMs no cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

Exibir entradas da tabela do host DNS (somente administradores de cluster)

As entradas da tabela de hosts DNS mapeiam nomes de host para endereços IP. É possível exibir os nomes de host e os nomes de alias e o endereço IP para o qual eles mapeiam para todos os SVMs em um cluster.

Passo

Exiba as entradas de nome de host para todos os SVMs usando o comando show de hosts dns de serviços vserver.

O exemplo a seguir exibe as entradas da tabela do host:

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- --------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os nomes de host são resolvidos usando servidores DNS externos.

Exibir configurações de domínio DNS

Você pode exibir a configuração do domínio DNS de uma ou mais máquinas virtuais de armazenamento (SVMs) no cluster para verificar se ela está configurada corretamente.

Passo

Exibindo as configurações do domínio DNS usando o `vserver services name-service dns show` comando.

O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

```
vserver services name-service dns show
                                                 Name
Vserver         State     Domains                Servers
--------------- --------- ---------------------- -------------
cluster-1        enabled   xyz.company.com         192.56.0.129,
                                                 192.56.0.130
vs1             enabled   xyz.company.com        192.56.0.129,
                                                 192.56.0.130
vs2             enabled   xyz.company.com        192.56.0.129,
                                                 192.56.0.130
vs3             enabled   xyz.company.com        192.56.0.129,
                                                 192.56.0.130
```

O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

Exibir informações sobre grupos de failover

Você pode exibir informações sobre grupos de failover, incluindo a lista de nós e portas em cada grupo de failover, se o failover está ativado ou desativado e o tipo de política de failover que está sendo aplicada a cada LIF.

Passos

1. Exiba as portas de destino para cada grupo de failover usando o `network interface failover-groups show` comando.

   O comando a seguir exibe informações sobre todos os grupos de failover em um cluster de dois nós:

```
network interface failover-groups show
                              Failover
Vserver        Group          Targets
-------------- -------------- ---------------------------------
Cluster
               Cluster
                              cluster1-01:e0a, cluster1-01:e0b,
                              cluster1-02:e0a, cluster1-02:e0b
vs1
               Default
                              cluster1-01:e0c, cluster1-01:e0d,
                              cluster1-01:e0e, cluster1-02:e0c,
                              cluster1-02:e0d, cluster1-02:e0e
```

2. Exiba as portas de destino e o domínio de broadcast para um grupo de failover específico usando o `network interface failover-groups show` comando.

   O comando a seguir exibe informações detalhadas sobre o grupo de failover data12 para SVM VS4:

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. Exiba as configurações de failover usadas por todos os LIFs usando o `network interface show` comando.

   O comando a seguir exibe a política de failover e o grupo de failover que está sendo usado por cada LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -------------------  ---------------------  --------------
Cluster   cluster1-01_clus_1  local-only             Cluster
Cluster   cluster1-01_clus_2  local-only             Cluster
Cluster   cluster1-02_clus_1  local-only             Cluster
Cluster   cluster1-02_clus_2  local-only             Cluster
cluster1  cluster_mgmt        broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1   local-only             Default
cluster1  cluster1-02_mgmt1   local-only             Default
vs1       data1               disabled               Default
vs3       data2               system-defined         group2
```

Exibir destinos de failover de LIF

Talvez seja necessário verificar se as políticas de failover e os grupos de failover de um LIF estão configurados corretamente. Para evitar a configuração incorreta das regras de failover, você pode exibir os destinos de failover para um único LIF ou para todos os LIFs.

Sobre esta tarefa

A exibição de destinos de failover de LIF permite verificar o seguinte:

- Se os LIFs são configurados com o grupo de failover correto e a política de failover
- Se a lista resultante de portas de destino de failover é apropriada para cada LIF
- Se o destino de failover de um LIF de dados não é uma porta de gerenciamento (e0M)

Passo

Exiba os destinos de failover de um LIF usando a `failover` opção `network interface show` do

comando.

O comando a seguir exibe informações sobre os destinos de failover para todos os LIFs em um cluster de dois nós. A `Failover Targets` linha mostra a lista (priorizada) de combinações de nó-porta para um determinado LIF.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

Exibir LIFs em uma zona de balanceamento de carga

Você pode verificar se uma zona de balanceamento de carga está configurada

corretamente exibindo todas as LIFs que pertencem a ela. Você também pode visualizar a zona de balanceamento de carga de um LIF específico ou as zonas de balanceamento de carga de todos os LIFs.

Passo

Exiba os LIFs e os detalhes de balanceamento de carga desejados usando um dos seguintes comandos

Para exibir…	Digite…
LIFs em uma determinada zona de balanceamento de carga	`network interface show -dns-zone zone_name` `zone_name` especifica o nome da zona de balanceamento de carga.
A zona de balanceamento de carga de um LIF específico	`network interface show -lif lif_name -fields dns-zone`
As zonas de balanceamento de carga de todos os LIFs	`network interface show -fields dns-zone`

Exemplos de exibição de zonas de balanceamento de carga para LIFs

O comando a seguir exibe os detalhes de todos os LIFs na zona de balanceamento de carga storage.company.com para SVM vs0:

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network           Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask      Node      Port    Home
--------- ---------- ---------- ----------------- --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

O comando a seguir exibe os detalhes da zona DNS do LIF data3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

O comando a seguir exibe a lista de todos os LIFs no cluster e suas zonas DNS correspondentes:

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

Exibir conexões do cluster no ONTAP

Você pode exibir todas as conexões ativas no cluster ou uma contagem de conexões ativas no nó por cliente, interface lógica, protocolo ou serviço. Também pode apresentar todas as ligações de audição no cluster.

Exibir conexões ativas pelo cliente (somente administradores de cluster)

Você pode exibir as conexões ativas por cliente para verificar o nó que um cliente específico está usando e para exibir possíveis desequilíbrios entre contagens de clientes por nó.

Sobre esta tarefa

A contagem de conexões ativas por cliente é útil nos seguintes cenários:

- Encontrando um nó ocupado ou sobrecarregado.
- Determinar por que o acesso de um cliente específico a um volume é lento.

  Você pode ver detalhes sobre o nó que o cliente está acessando e compará-lo com o nó no qual o volume reside. Se o acesso ao volume exigir a travessia da rede do cluster, os clientes podem ter um desempenho reduzido devido ao acesso remoto ao volume em um nó remoto substituído.

- Verificar se todos os nós estão sendo usados igualmente para acesso aos dados.
- Encontrando clientes que têm um número inesperadamente alto de conexões.
- Verificando se certos clientes têm conexões com um nó.

Passo

Exibir uma contagem das conexões ativas por cliente em um nó usando o `network connections active show-clients` comando.

Saiba mais sobre o comando link:http://docs.NetApp.com/US-en/ONTAP-cli/network-connections-active-show-clients.html[`network connections active show-clients` em referência de comando ONTAP.

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

Exibir conexões ativas por protocolo (somente administradores de cluster)

É possível exibir uma contagem das conexões ativas por protocolo (TCP ou UDP) em um nó para comparar o uso de protocolos dentro do cluster.

Sobre esta tarefa

A contagem de conexões ativas por protocolo é útil nos seguintes cenários:

- Encontrando os clientes UDP que estão perdendo sua conexão.

  Se um nó estiver próximo ao limite de conexão, os clientes UDP serão os primeiros a serem descartados.

- Verificar se não estão a ser utilizados outros protocolos.

Passo

Exibir uma contagem das conexões ativas por protocolo em um nó usando o `network connections active show-protocols` comando.

Para obter mais informações sobre esse comando, consulte a página man.

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

Exibir conexões ativas por serviço (somente administradores de cluster)

É possível exibir uma contagem das conexões ativas por tipo de serviço (por exemplo, por NFS, SMB, montagem etc.) para cada nó em um cluster. Isso é útil para comparar o uso de serviços no cluster, o que ajuda a determinar a carga de trabalho principal de um nó.

Sobre esta tarefa

A contagem de conexões ativas por serviço é útil nos seguintes cenários:

- Verificar se todos os nós estão sendo usados para os serviços apropriados e se o balanceamento de carga para esse serviço está funcionando.
- Verificar se não estão a ser utilizados outros serviços. Exibir uma contagem das conexões ativas por serviço em um nó usando o `network connections active show-services` comando.

Para obter mais informações sobre esse comando, consulte a página man: "Referência do comando ONTAP"

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

Exibir conexões ativas por LIF em um nó e SVM

É possível exibir uma contagem de conexões ativas para cada LIF, por nó e máquina virtual de armazenamento (SVM), para visualizar desequilíbrios de conexão entre LIFs no cluster.

Sobre esta tarefa

A contagem de conexões ativas por LIF é útil nos seguintes cenários:

- Encontrando um LIF sobrecarregado comparando o número de conexões em cada LIF.
- Verificando se o balanceamento de carga DNS está funcionando para todas as LIFs de dados.
- Comparando o número de conexões com os vários SVMs para encontrar os SVMs que são mais usados.

Passo

Exiba uma contagem de conexões ativas para cada LIF por SVM e nó usando o `network connections active show-lifs` comando.

Para obter mais informações sobre esse comando, consulte a página man: "Referência do comando ONTAP"

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

Exibir conexões ativas em um cluster

Você pode exibir informações sobre as conexões ativas em um cluster para exibir o LIF, a porta, o host remoto, o serviço, as máquinas virtuais de armazenamento (SVMs) e o protocolo usado por conexões individuais.

Sobre esta tarefa

Visualizar as conexões ativas em um cluster é útil nos seguintes cenários:

- Verificar se clientes individuais estão usando o protocolo e o serviço corretos no nó correto.
- Se um cliente estiver tendo problemas para acessar dados usando uma certa combinação de nó, protocolo e serviço, você pode usar este comando para encontrar um cliente semelhante para comparação de configuração ou rastreamento de pacotes.

Passo

Exiba as conexões ativas em um cluster usando o `network connections active show` comando.

Para obter mais informações sobre esse comando, consulte a página man: "Referência do comando ONTAP".

O comando a seguir mostra as conexões ativas no nó node1:

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

O comando a seguir mostra as conexões ativas no SVM VS1:

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

Exibir conexões de escuta em um cluster

Você pode exibir informações sobre as conexões de escuta em um cluster para exibir os LIFs e as portas que estão aceitando conexões para um determinado protocolo e serviço.

Sobre esta tarefa

Visualizar as conexões de escuta em um cluster é útil nos seguintes cenários:

- Verificar se o protocolo ou serviço desejado está escutando em um LIF se as conexões do cliente a esse LIF falharem consistentemente.
- Verificar se um ouvinte UDP/rclopcp é aberto em cada LIF de cluster se o acesso remoto de dados a um volume em um nó por meio de um LIF em outro nó falhar.
- Verificar se um ouvinte UDP/rclopcp é aberto em cada LIF de cluster se as transferências SnapMirror entre dois nós no mesmo cluster falharem.
- Verificando se um ouvinte TCP/ctlopcp é aberto em cada LIF entre clusters se as transferências SnapMirror entre dois nós em clusters diferentes falharem.

Passo

Exiba as conexões de escuta por nó usando o `network connections listening show` comando.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

Comandos para diagnosticar problemas de rede

Pode diagnosticar problemas na rede utilizando comandos como `ping`, `traceroute`, `ndp`, e `tcpdump`. Você também pode usar comandos como `ping6` e `traceroute6` para diagnosticar problemas do IPv6.

Se você quiser…	Digite este comando…
Teste se o nó pode alcançar outros hosts em sua rede	`network ping`
Teste se o nó pode alcançar outros hosts em sua rede IPv6	`network ping6`
Trace a rota que os pacotes IPv4 levam para um nó de rede	`network traceroute`
Trace a rota que os pacotes IPv6 levam para um nó de rede	`network traceroute6`
Gerenciar o Neighbor Discovery Protocol (NDP)	`network ndp`
Exibir estatísticas sobre pacotes recebidos e enviados em uma interface de rede especificada ou em todas as interfaces de rede	`run -node` *`node_name`* `ifstat` **Nota**: Este comando está disponível no nodeshell.
Exiba informações sobre dispositivos vizinhos que são descobertos de cada nó e porta no cluster, incluindo o tipo de dispositivo remoto e a plataforma do dispositivo	`network device-discovery show`
Visualizar os vizinhos CDP do nó (o ONTAP suporta apenas CDPv1 anúncios)	`run -node` *`node_name`* `cdpd show-neighbors` **Nota**: Este comando está disponível no nodeshell.

Rastreie os pacotes que são enviados e recebidos na rede	`network tcpdump start -node` *`node-name`* `-port` *`port_name`* **Nota**: Este comando está disponível no nodeshell.
Meça a latência e a taxa de transferência entre clusters ou nós entre clusters	`network test -path -source-node` *`source_nodename local`* `-destination -cluster` *`destination_clustername`* `-destination-node` *`destination_nodename`* `-session-type` *`Default`*, *`AsyncMirrorLocal`*, *`AsyncMirrorRemote`*, *`SyncMirrorRemote`*, `or` *`RemoteDataTransfer`* Para obter mais informações, consulte "Gerenciamento de desempenho".

Para obter mais informações sobre esses comandos, consulte "Referência do comando ONTAP" .

Exibir conetividade de rede com protocolos de descoberta de vizinhos

Exibir conetividade de rede com protocolos de descoberta de vizinhos

Em um data center, você pode usar protocolos de descoberta de vizinhos para visualizar a conetividade de rede entre um par de sistemas físicos ou virtuais e suas interfaces de rede. O ONTAP oferece suporte a dois protocolos de descoberta de vizinhos: O Protocolo de descoberta de Cisco (CDP) e o Protocolo de descoberta de camada de enlace (LLDP).

Os protocolos de descoberta de vizinhos permitem que você descubra e visualize automaticamente informações sobre dispositivos habilitados para protocolo diretamente conetados em uma rede. Cada dispositivo anuncia informações de identificação, recursos e conetividade. Essas informações são transmitidas em quadros Ethernet para um endereço MAC multicast e são recebidas por todos os dispositivos habilitados para protocolo vizinhos.

Para que dois dispositivos se tornem vizinhos, cada um deve ter um protocolo ativado e configurado corretamente. A funcionalidade do protocolo Discovery está limitada a redes diretamente ligadas. Os vizinhos podem incluir dispositivos habilitados para protocolo, como switches, roteadores, bridges e assim por diante. O ONTAP suporta dois protocolos de descoberta de vizinhos, que podem ser usados individualmente ou em conjunto.

Protocolo de descoberta de Cisco (CDP)

O CDP é um protocolo de camada de link proprietário desenvolvido pela Cisco Systems. Ele é habilitado por padrão no ONTAP para portas de cluster, mas deve ser habilitado explicitamente para portas de dados.

Protocolo de descoberta de camada de link (LLDP)

LLDP é um protocolo neutro para fornecedores especificado no documento padrões IEEE 802,1AB.3. Ele deve ser habilitado explicitamente para todas as portas.

Use o CDP para detetar conetividade de rede

O uso do CDP para detetar a conetividade de rede consiste em revisar considerações de implantação, habilitá-lo em portas de dados, visualizar dispositivos vizinhos e ajustar os

valores de configuração do CDP conforme necessário. O CDP é ativado por padrão nas portas do cluster.

O CDP também deve ser ativado em todos os switches e roteadores antes que as informações sobre dispositivos vizinhos possam ser exibidas.

Lançamento do ONTAP	Descrição
9.10.1 e anteriores	O CDP também é usado pelo monitor de integridade do switch de cluster para descobrir automaticamente seus switches de rede de gerenciamento e cluster.
9.11.1 e mais tarde	O CDP também é usado pelo monitor de integridade do switch de cluster para descobrir automaticamente o cluster, o armazenamento e os switches de rede de gerenciamento.

Informações relacionadas

"Administração do sistema"

Considerações para usar CDP

Por padrão, os dispositivos compatíveis com CDP enviam CDPv2 anúncios. Os dispositivos compatíveis com CDP enviam CDPv1 anúncios apenas quando recebem CDPv1 anúncios. O ONTAP suporta apenas CDPv1. Portanto, quando um nó ONTAP envia anúncios CDPv1, os dispositivos vizinhos compatíveis com CDP enviam CDPv1 anúncios.

Você deve considerar as seguintes informações antes de ativar o CDP em um nó:

- O CDP é suportado para todas as portas.
- Os anúncios CDP são enviados e recebidos por portas que estão no estado up.
- O CDP deve estar ativado nos dispositivos de transmissão e receção para enviar e receber anúncios CDP.
- Os anúncios CDP são enviados em intervalos regulares e você pode configurar o intervalo de tempo.
- Quando os endereços IP são alterados para um LIF, o nó envia as informações atualizadas no próximo anúncio do CDP.
- ONTAP 9.10,1 e anteriores:
  - O CDP está sempre ativado nas portas do cluster.
  - O CDP está desativado, por padrão, em todas as portas que não sejam de cluster.
- ONTAP 9.11,1 e posterior:
  - O CDP está sempre ativado em portas de cluster e armazenamento.
  - O CDP está desativado, por padrão, em todas as portas que não sejam de cluster e não de armazenamento.

> Às vezes, quando os LIFs são alterados no nó, as informações do CDP não são atualizadas no lado do dispositivo recetor (por exemplo, um switch). Se você encontrar esse problema, você deve configurar a interface de rede do nó para o status de baixo e, em seguida, para o status de cima.

- Apenas endereços IPv4 são anunciados em anúncios CDP.

- Para portas de rede físicas com VLANs, todas as LIFs configuradas nas VLANs nessa porta são anunciadas.
- Para portas físicas que fazem parte de um grupo de interfaces, todos os endereços IP configurados nesse grupo de interfaces são anunciados em cada porta física.
- Para um grupo de interfaces que hospeda VLANs, todas as LIFs configuradas no grupo de interfaces e as VLANs são anunciadas em cada uma das portas de rede.
- Devido aos pacotes CDP serem restritos a não mais de 1500 bytes, em portas configuradas com um grande número de LIFs, apenas um subconjunto desses endereços IP pode ser relatado no switch adjacente.

Ativar ou desativar o CDP

Para descobrir e enviar anúncios para dispositivos vizinhos compatíveis com CDP, o CDP deve estar ativado em cada nó do cluster.

Por padrão no ONTAP 9.10,1 e versões anteriores, o CDP é ativado em todas as portas de cluster de um nó e desativado em todas as portas que não sejam de cluster de um nó.

Por padrão no ONTAP 9.11,1 e posterior, o CDP é ativado em todos os clusters e portas de armazenamento de um nó e desativado em todas as portas que não sejam de cluster e não de armazenamento de um nó.

Sobre esta tarefa

A `cdpd.enable` opção controla se o CDP está ativado ou desativado nas portas de um nó:

- Para o ONTAP 9.10,1 e anterior, o ON ativa o CDP em portas que não sejam de cluster.
- Para o ONTAP 9.11,1 e posterior, o ON ativa o CDP em portas que não sejam de cluster e que não sejam de armazenamento.
- Para ONTAP 9.10,1 e anteriores, Desativar desativa o CDP em portas que não sejam de cluster; não é possível desativar o CDP em portas de cluster.
- Para o ONTAP 9.11,1 e posterior, Desativar desativa o CDP em portas que não sejam de cluster e que não sejam de armazenamento; não é possível desativar o CDP em portas de cluster.

Quando o CDP está desativado em uma porta que está conetada a um dispositivo compatível com CDP, o tráfego de rede pode não ser otimizado.

Passos

1. Exibir a configuração atual de CDP para um nó ou para todos os nós em um cluster:

Para ver a definição CDP de…	Digite…
Um nó	`run - node <node_name> options cdpd.enable`
Todos os nós em um cluster	`options cdpd.enable`

2. Ative ou desative o CDP em todas as portas de um nó ou em todas as portas de todos os nós de um cluster:

Para ativar ou desativar o CDP em…	Digite…

Um nó	`run -node node_name options cdpd.enable {on or off}`
Todos os nós em um cluster	`options cdpd.enable {on or off}`

Exibir informações sobre o vizinho CDP

Você pode exibir informações sobre os dispositivos vizinhos que estão conetados a cada porta dos nós do cluster, desde que a porta esteja conetada a um dispositivo compatível com CDP. Você pode usar o `network device-discovery show -protocol cdp` comando para exibir informações de vizinhos.

Sobre esta tarefa

No ONTAP 9.10,1 e anterior, como o CDP está sempre ativado para portas de cluster, as informações de vizinhos do CDP são sempre exibidas para essas portas. O CDP deve estar habilitado em portas que não sejam de cluster para que as informações de vizinhos apareçam para essas portas.

No ONTAP 9.11,1 e posterior, uma vez que o CDP está sempre ativado para portas de cluster e armazenamento, as informações do vizinho CDP são sempre exibidas para essas portas. O CDP deve estar habilitado em portas que não sejam de cluster e não de armazenamento para que as informações de vizinhos apareçam para essas portas.

Passo

Exiba informações sobre todos os dispositivos compatíveis com CDP conetados às portas em um nó no cluster:

```
network device-discovery show -node node -protocol cdp
```

O comando a seguir mostra os vizinhos que estão conetados às portas no nó sti2650-212:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

A saída lista os dispositivos Cisco que estão conetados a cada porta do nó especificado.

Configure o tempo de espera para mensagens CDP

Tempo de espera é o período de tempo durante o qual os anúncios CDP são armazenados em cache em dispositivos compatíveis com CDP vizinhos. O tempo de espera é anunciado em cada pacote CDPv1 e é atualizado sempre que um pacote CDPv1 é recebido por um nó.

- O valor `cdpd.holdtime` da opção deve ser definido com o mesmo valor em ambos os nós de um par de HA.
- O valor de tempo de retenção padrão é de 180 segundos, mas você pode inserir valores que variam de 10 segundos a 255 segundos.
- Se um endereço IP for removido antes que o tempo de espera expire, as informações do CDP serão armazenadas em cache até que o tempo de espera expire.

Passos

1. Exibir o tempo atual de retenção do CDP para um nó ou para todos os nós em um cluster:

Para ver o tempo de espera de…	Digite…
Um nó	`run -node node_name options cdpd.holdtime`

Todos os nós em um cluster	`options cdpd.holdtime`

2. Configure o tempo de retenção do CDP em todas as portas de um nó ou em todas as portas de todos os nós em um cluster:

Para definir o tempo de espera em…	Digite…
Um nó	`run -node node_name options cdpd.holdtime holdtime`
Todos os nós em um cluster	`options cdpd.holdtime holdtime`

Defina o intervalo para enviar anúncios CDP

Os anúncios do CDP são enviados para vizinhos do CDP em intervalos periódicos. Você pode aumentar ou diminuir o intervalo para enviar anúncios CDP dependendo do tráfego de rede e alterações na topologia da rede.

- O valor `cdpd.interval` da opção deve ser definido com o mesmo valor em ambos os nós de um par de HA.
- O intervalo padrão é de 60 segundos, mas você pode inserir um valor de 5 segundos a 900 segundos.

Passos

1. Exibir o intervalo de tempo atual do anúncio do CDP para um nó ou para todos os nós em um cluster:

Para ver o intervalo para…	Digite…
Um nó	`run -node node_name options cdpd.interval`
Todos os nós em um cluster	`options cdpd.interval`

2. Configure o intervalo para enviar anúncios CDP para todas as portas de um nó ou para todas as portas de todos os nós em um cluster:

Para definir o intervalo para…	Digite…
Um nó	`run -node node_name options cdpd.interval interval`
Todos os nós em um cluster	`options cdpd.interval interval`

Exibir ou limpar estatísticas CDP

Você pode exibir as estatísticas do CDP para as portas de cluster e não cluster em cada nó para detetar possíveis problemas de conetividade de rede. As estatísticas de CDP são cumulativas a partir do momento em que foram eliminadas pela última vez.

Sobre esta tarefa

No ONTAP 9.10,1 e anterior, como o CDP está sempre ativado para portas, as estatísticas CDP são sempre exibidas para o tráfego nessas portas. O CDP deve estar ativado nas portas para que as estatísticas apareçam para essas portas.

No ONTAP 9.11,1 e posterior, como o CDP está sempre ativado para portas de cluster e armazenamento, as estatísticas CDP são sempre exibidas para o tráfego nessas portas. O CDP deve estar habilitado em portas que não sejam de cluster ou não de armazenamento para que as estatísticas apareçam para essas portas.

Passo

Exibir ou limpar as estatísticas CDP atuais para todas as portas em um nó:

Se você quiser…	Digite…
Veja as estatísticas do CDP	`run -node node_name cdpd show-stats`
Limpe as estatísticas do CDP	`run -node node_name cdpd zero-stats`

Exemplo de estatísticas de exibição e limpeza

O comando a seguir mostra as estatísticas do CDP antes de serem apagadas. A saída exibe o número total de pacotes que foram enviados e recebidos desde a última vez que as estatísticas foram apagadas.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

O seguinte comando limpa as estatísticas CDP:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:            0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

Depois que as estatísticas são apagadas, elas começam a se acumular após o próximo anúncio do CDP ser enviado ou recebido.

Conexão a switches Ethernet que não suportam CDP

Vários switches de fornecedores não suportam CDP. Consulte o artigo da base de dados de Conhecimento "A deteção de dispositivo ONTAP mostra nós em vez do switch" para obter mais detalhes.

Existem duas opções para resolver este problema:

- Desative o CDP e ative o LLDP, se suportado. "Use o LLDP para detetar conetividade de rede"Consulte para obter mais detalhes.
- Configure um filtro de pacote de endereços MAC nos switches para soltar anúncios CDP.

Use o LLDP para detetar conetividade de rede

O uso do LLDP para detetar a conetividade de rede consiste em revisar considerações de implantação, habilitá-lo em todas as portas, visualizar dispositivos vizinhos e ajustar os valores de configuração do LLDP conforme necessário.

O LLDP também deve ser ativado em qualquer switch e roteador antes que as informações sobre dispositivos vizinhos possam ser exibidas.

O ONTAP relata atualmente as seguintes estruturas de tipo-comprimento-valor (TLVs):

- ID do chassis
- ID da porta
- Tempo para viver (TTL)
- Nome do sistema

  O nome do sistema TLV não é enviado em dispositivos CNA.

Certos adaptadores de rede convergidos (CNAs), como o adaptador X1143 e as portas integradas UTA2, contêm suporte de descarga para LLDP:

- A descarga LLDP é usada para Data Center Bridging (DCB).
- As informações exibidas podem diferir entre o cluster e o switch.

  Os dados de ID do chassi e ID da porta exibidos pelo switch podem ser diferentes para portas CNA e não CNA.

Por exemplo:

- Para portas não CNA:
  - O ID do chassis é um endereço MAC fixo de uma das portas no nó
  - ID da porta é o nome da porta correspondente no nó
- Para portas CNA:
  - ID do chassis e ID da porta são os endereços MAC das respetivas portas no nó.

No entanto, os dados exibidos pelo cluster são consistentes para esses tipos de portas.

A especificação LLDP define o acesso às informações coletadas por meio de um MIB SNMP. No entanto, o ONTAP não suporta atualmente o MIB LLDP.

Ativar ou desativar o LLDP

Para descobrir e enviar anúncios para dispositivos vizinhos compatíveis com LLDP, o LLDP deve estar habilitado em cada nó do cluster. A partir do ONTAP 9.7, o LLDP é ativado em todas as portas de um nó por padrão.

Sobre esta tarefa

Para o ONTAP 9.10,1 e anterior, a `lldp.enable` opção controla se o LLDP está ativado ou desativado nas portas de um nó:

- `on` Ativa o LLDP em todas as portas.
- `off` Desativa o LLDP em todas as portas.

Para o ONTAP 9.11,1 e posterior, a `lldp.enable` opção controla se o LLDP está ativado ou desativado nas portas que não são de cluster e não são de storage de um nó:

- `on` Habilita o LLDP em todas as portas que não são de cluster e não são de storage.
- `off` Desativa o LLDP em todas as portas que não sejam de cluster e não de armazenamento.

Passos

1. Exibir a configuração atual de LLDP para um nó ou para todos os nós em um cluster:
   - Nó único: `run -node node_name options lldp.enable`
   - Todos os nós: Opções `lldp.enable`
2. Ative ou desative o LLDP em todas as portas de um nó ou em todas as portas de todos os nós em um cluster:

Para ativar ou desativar o LLDP em…	Digite…

Um nó	`run -node node_name options lldp.enable {on
off}`	Todos os nós em um cluster
`options lldp.enable {on	off}`

- Nó único:

```
run -node node_name options lldp.enable {on|off}
```

- Todos os nós:

```
options lldp.enable {on|off}
```

Ver informações do vizinho LLDP

Você pode exibir informações sobre os dispositivos vizinhos que estão conetados a cada porta dos nós do cluster, desde que a porta esteja conetada a um dispositivo compatível com LLDP. Você usa o comando network device-Discovery show para exibir informações de vizinhos.

Passo

1. Exiba informações sobre todos os dispositivos compatíveis com LLDP conetados às portas em um nó no cluster:

```
network device-discovery show -node node -protocol lldp
```

O comando a seguir mostra os vizinhos que estão conetados às portas no cluster de nó-1_01. A saída lista os dispositivos habilitados para LLDP que estão conetados a cada porta do nó especificado. Se a `-protocol` opção for omitida, a saída também lista dispositivos habilitados para CDP.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Ajuste o intervalo para transmitir anúncios LLDP

Anúncios LLDP são enviados para vizinhos LLDP em intervalos periódicos. Você pode aumentar ou diminuir o intervalo para enviar anúncios LLDP dependendo do tráfego de rede e alterações na topologia da rede.

Sobre esta tarefa

O intervalo padrão recomendado pelo IEEE é de 30 segundos, mas você pode inserir um valor de 5 segundos a 300 segundos.

Passos

1. Exibir o intervalo de tempo de anúncio LLDP atual para um nó ou para todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - Todos os nós:

     ```
     options lldp.xmit.interval
     ```

2. Ajuste o intervalo para o envio de anúncios LLDP para todas as portas de um nó ou para todas as portas de todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - Todos os nós:

     ```
     options lldp.xmit.interval <interval>
     ```

Ajuste o valor time-to-live para anúncios LLDP

Time-to-Live (TTL) é o período de tempo para o qual os anúncios LLDP são armazenados em cache em dispositivos compatíveis com LLDP vizinhos. TTL é anunciado em cada pacote LLDP e é atualizado sempre que um pacote LLDP é recebido por um nó. TTL pode ser modificado em quadros LLDP de saída.

Sobre esta tarefa

- TTL é um valor calculado, o produto do intervalo de transmissão (`lldp.xmit.interval`) e o multiplicador de retenção (`lldp.xmit.hold`) mais um.
- O valor multiplicador de retenção padrão é 4, mas você pode inserir valores que variam de 1 a 100.
- O TTL padrão é, portanto, 121 segundos, como recomendado pelo IEEE, mas ajustando os valores do multiplicador de intervalo de transmissão e retenção, você pode especificar um valor para quadros de saída de 6 segundos a 30001 segundos.
- Se um endereço IP for removido antes do TTL expirar, as informações do LLDP serão armazenadas em cache até que o TTL expire.

Passos

1. Exibir o valor multiplicador de retenção atual para um nó ou para todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - Todos os nós:

     ```
     options lldp.xmit.hold
     ```

2. Ajuste o valor multiplicador de retenção em todas as portas de um nó ou em todas as portas de todos os nós em um cluster:
   - Nó único:

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - Todos os nós:

     ```
     options lldp.xmit.hold <hold_value>
     ```

Exibir ou limpar estatísticas LLDP

Você pode exibir as estatísticas do LLDP para as portas de cluster e não cluster em cada nó para detetar possíveis problemas de conetividade de rede. As estatísticas LLDP são cumulativas a partir do momento em que foram eliminadas pela última vez.

Sobre esta tarefa

Para o ONTAP 9.10,1 e versões anteriores, como o LLDP está sempre ativado para portas de cluster, as estatísticas do LLDP são sempre exibidas para o tráfego nessas portas. O LLDP deve estar habilitado em portas que não sejam de cluster para que as estatísticas apareçam para essas portas.

Para o ONTAP 9.11,1 e posterior, como o LLDP está sempre ativado para portas de cluster e armazenamento, as estatísticas do LLDP são sempre exibidas para o tráfego nessas portas. O LLDP deve estar habilitado em portas que não sejam de cluster e não de storage para que as estatísticas apareçam para essas portas.

Passo

Exibir ou limpar as estatísticas LLDP atuais para todas as portas em um nó:

Se você quiser…	Digite…
Veja as estatísticas do LLDP	`run -node node_name lldp stats`
Limpe as estatísticas do LLDP	`run -node node_name lldp stats -z`

Mostrar e limpar o exemplo de estatísticas

O comando a seguir mostra as estatísticas LLDP antes de serem limpas. A saída exibe o número total de pacotes que foram enviados e recebidos desde a última vez que as estatísticas foram apagadas.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

O comando a seguir limpa as estatísticas LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

Depois que as estatísticas são apagadas, elas começam a se acumular após o próximo anúncio LLDP ser enviado ou recebido.

Gerenciamento de storage nas

Gerenciar protocolos nas com o System Manager

Visão geral do gerenciamento nas com o System Manager

Os tópicos nesta seção mostram como configurar e gerenciar ambientes nas com o System Manager no ONTAP 9.7 e versões posteriores.

Se você estiver usando o gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), consulte estes tópicos:

- "Visão geral da configuração NFS"
- "Visão geral da configuração SMB"

O System Manager é compatível com fluxos de trabalho para:

- Configuração inicial de clusters que você pretende usar para serviços de arquivos nas.
- Provisionamento de volume adicional para necessidades dinâmicas de storage.
- Configuração e manutenção para instalações de autenticação e segurança padrão do setor.

Com o System Manager, você pode gerenciar serviços nas no nível de componente:

- Protocolos - NFS, SMB ou ambos (multiprotocolo nas)
- Serviços de nomes - DNS, LDAP e NIS
- Switch do serviço de nomes
- Segurança Kerberos e TLS
- Exportações e ações
- Qtrees
- Mapeamento de nomes de usuários e grupos

Provisione storage NFS para datastores VMware

Antes de usar o console de storage virtual para VMware vSphere (VSC) para provisionar volumes NFS em um sistema de storage baseado em ONTAP para hosts ESXi, ative o NFS usando o System Manager para ONTAP 9.7 ou posterior.

Depois de criar um "VM de storage habilitada por NFS" no System Manager, você provisiona volumes NFS e gerencia armazenamentos de dados usando o VSC.

A partir do VSC 7,0, o VSC faz parte "Ferramentas do ONTAP para o dispositivo virtual VMware vSphere" do , que inclui o VSC, o provedor vStorage APIs for Storage Awareness (VASA) e o Storage Replication Adapter (SRA) para os recursos do VMware vSphere.

Certifique-se de que verifica o "Matriz de interoperabilidade do NetApp" para confirmar a compatibilidade entre as versões atuais do ONTAP e do VSC.

Para configurar o acesso NFS para hosts ESXi em armazenamentos de dados usando o System Manager

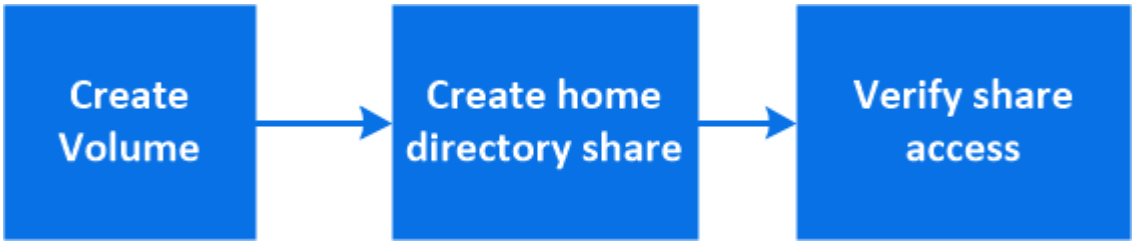
Classic (para ONTAP 9.7 e versões anteriores), consulte "Configuração NFS para ESXi usando visão geral do VSC"

Para obter mais informações, consulte "TR-4597: VMware vSphere for ONTAP" e a documentação da versão do VSC.

Provisione storage nas para diretórios base

Crie volumes para fornecer armazenamento para diretórios base usando o protocolo SMB.

Este procedimento cria novos volumes para diretórios base em um "VM de storage habilitada para SMB existente". Você pode aceitar padrões de sistemas ao configurar volumes ou especificar configurações personalizadas.



Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance, criar o FlexGroup volumes. Consulte também "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup".

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Passos

1. Adicione um novo volume em uma VM de storage habilitada para SMB.
   a. Selecione **armazenamento > volumes** e clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Apenas as VMs de armazenamento configuradas com o protocolo SMB são listadas. Se apenas uma VM de armazenamento configurada com o protocolo SMB estiver disponível, o campo **Storage VM** não será exibido.

      - Se você clicar em **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.
      - Você pode clicar em **mais opções** para personalizar a configuração do volume para ativar serviços como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.
2. clique em **armazenamento > compartilhamentos**, clique em **Adicionar** e selecione **Home Directory**.
3. Em um cliente Windows, faça o seguinte para verificar se o compartilhamento está acessível.
   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\<SMB_Server_Name>\<Share_Name>`

      Se o nome do compartilhamento foi criado com variáveis (%W, %d ou %u), certifique-se de testar o acesso com um nome resolvido.

b. Na unidade recém-criada, crie um arquivo de teste e exclua o arquivo.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

  - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
  - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
  - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado, poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**) no qual deseja colocar o volume que está criando.

    Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.
- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

  Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.
- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne Etapa 2 no fluxo de trabalhoao provisionamento completo para diretórios base.

Provisione storage nas para servidores Linux usando NFS

Crie volumes para fornecer storage para servidores Linux usando o protocolo NFS com o ONTAP System Manager (9,7 e posterior).

Este procedimento cria novos volumes em um "VM de storage habilitada por NFS existente". Você pode aceitar padrões do sistema ao configurar volumes ou especificar configurações personalizadas.

Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance, criar o FlexGroup volumes. Consulte também "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup".

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Se quiser obter detalhes sobre a gama de capacidades do protocolo NFS da ONTAP, consulte o "Visão geral de referência de NFS".

Passos

1. Adicionar um novo volume em uma VM de storage habilitada por NFS.
   a. Clique em **Storage > volumes** e, em seguida, clique em **Add**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Somente as VMs de storage configuradas com o protocolo NFS são listadas. Se apenas uma VM de armazenamento configurada com o protocolo SMB estiver disponível, o campo **Storage VM** não será exibido.

      - Se você clicar em **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.

        A política de exportação padrão concede acesso total a todos os usuários.

      - Você pode clicar em **mais opções** para personalizar a configuração do volume para ativar serviços como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.
2. em um cliente Linux, faça o seguinte para verificar o acesso.
   a. Crie e monte o volume usando a interface de rede da VM de armazenamento.
   b. No volume recém-montado, crie um arquivo de teste, escreva texto nele e exclua o arquivo.

   Depois de verificar o acesso, você pode "restringir o acesso do cliente com a política de exportação do volume" e definir qualquer propriedade e permissões UNIX desejadas no volume montado.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

  - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
  - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
  - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado, poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**)

no qual deseja colocar o volume que está criando.

Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.

- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

  Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.

- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne ao Etapa 2 no fluxo de trabalhoprovisionamento completo para servidores Linux usando NFS.

Outras maneiras de fazer isso em ONTAP

Para executar esta tarefa com…	Consulte…
Gerenciador de sistema Clássico (ONTAP 9 .7 e anteriores)	"Visão geral da configuração NFS"
A interface de linha de comando (CLI) do ONTAP	"Visão geral da configuração de NFS com a CLI"

Gerenciar o acesso usando políticas de exportação

Habilite o acesso de cliente Linux a servidores NFS usando políticas de exportação.

Este procedimento cria ou modifica políticas de exportação para um "VM de storage habilitada por NFS existente".

Passos

1. No System Manager, clique em **Storage** > **volumes**.
2. Clique em um volume habilitado para NFS e clique em **More**.
3. Clique em **Editar política de exportação** e, em seguida, clique em **Selecionar uma política existente** ou em **Adicionar uma nova política**.

Provisione storage nas para servidores Windows usando SMB

Crie volumes para fornecer storage para servidores Windows usando o protocolo SMB usando o Gerenciador de sistemas, que está disponível com o ONTAP 9.7 e posterior.

Esse procedimento cria novos volumes em um "VM de storage habilitada para SMB existente" e cria um compartilhamento para o diretório raiz de volume (/). Você pode aceitar padrões de sistemas ao configurar volumes ou especificar configurações personalizadas. Após a configuração inicial do SMB, você também pode criar compartilhamentos adicionais e modificar suas propriedades.

Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance,

criar o FlexGroup volumes. Consulte também "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup".

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Se pretender obter detalhes sobre a gama de capacidades do protocolo SMB do ONTAP, consulte o "Visão geral de referência SMB".

Antes de começar

- A partir do ONTAP 9.13,1, você pode habilitar a análise de capacidade e o acompanhamento de atividades por padrão em novos volumes. No System Manager, você pode gerenciar as configurações padrão no nível de cluster ou VM de armazenamento. Para obter mais informações, "Ative a análise do sistema de ficheiros"consulte .

Passos

1. Adicione um novo volume em uma VM de storage habilitada para SMB.
   a. Clique em **Storage > volumes** e, em seguida, clique em **Add**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Apenas as VMs de armazenamento configuradas com o protocolo SMB são listadas. Se apenas uma VM de armazenamento configurada com o protocolo SMB estiver disponível, o campo **Storage VM** não será exibido.

      - Se você selecionar **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.
      - Você pode selecionar **mais opções** para personalizar a configuração do volume para ativar serviços como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.
2. mude para um cliente Windows para verificar se o compartilhamento está acessível.
   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\_SMB_Server_Name__Share_Name_`
   b. Na unidade recém-criada, crie um arquivo de teste, escreva texto para ele e exclua o arquivo.

Depois de verificar o acesso, você pode restringir o acesso do cliente com a ACL de compartilhamento e definir as propriedades de segurança desejadas na unidade mapeada. Consulte "Crie um compartilhamento SMB" para obter mais informações.

Adicionar ou modificar compartilhamentos

Você pode adicionar compartilhamentos adicionais após a configuração inicial do SMB. Os compartilhamentos são criados com valores e propriedades padrão que você selecionar. Estes podem ser modificados mais tarde.

Você pode definir as seguintes propriedades de compartilhamento ao configurar um compartilhamento:

- Permissões de acesso
- Compartilhar propriedades
  - Ative a disponibilidade contínua para compartilhamentos que contêm dados Hyper-V e SQL Server sobre SMB (começando com ONTAP 9.10,1). Veja também:

        - "Requisitos de compartilhamento continuamente disponíveis para Hyper-V sobre SMB"
        - "Requisitos de compartilhamento continuamente disponíveis para SQL Server sobre SMB"
    - Criptografe dados com SMB 3,0 enquanto acessa esse compartilhamento.

Após a configuração inicial, você também pode modificar estas propriedades:

- Links simbólicos
    - Ative ou desative links simbólicos e widelinks
- Compartilhar propriedades
    - Permitir que os clientes acessem o diretório cópias Snapshot.
    - Ative os oplocks, permitindo que os clientes bloqueiem arquivos e armazenem conteúdo em cache localmente (padrão).
    - Ative a enumeração baseada em acesso (ABE) para exibir recursos compartilhados com base nas permissões de acesso do usuário.

Procedimentos

Para adicionar um novo compartilhamento em um volume habilitado para SMB, clique em **armazenamento > compartilhamentos**, clique em **Adicionar** e selecione **compartilhar**.

Para modificar um compartilhamento existente, clique em **armazenamento > compartilhamentos** e, em seguida, clique em ⋮ e selecione **Editar**.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

    - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
    - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
    - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado, poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**) no qual deseja colocar o volume que está criando.

      Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.

- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.

- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne Etapa 2 no fluxo de trabalhoao provisionamento completo para servidores Windows usando SMB.

Outras maneiras de fazer isso em ONTAP

Para executar esta tarefa com…	Consulte…
Gerenciador de sistema Clássico (ONTAP 9 .7 e anteriores)	"Visão geral da configuração SMB"
A interface da linha de comando ONTAP	"Visão geral da configuração SMB com a CLI"

Provisionar storage nas para Windows e Linux usando NFS e SMB

Crie volumes para fornecer storage para clientes usando o protocolo NFS ou SMB.

Este procedimento cria novos volumes em um "VM de storage existente habilitada para protocolos NFS e SMB".

O protocolo NFS geralmente é usado em ambientes Linux. O protocolo SMB é geralmente usado em ambientes Windows. No entanto, tanto o NFS como o SMB podem ser usados com Linux ou Windows.

Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance, criar o FlexGroup volumes. "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup"Consulte .

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Passos

1. Adicione um novo volume em uma VM de storage habilitada para NFS e SMB.

   a. Clique em **Storage > volumes** e, em seguida, clique em **Add**.

   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Somente as VMs de storage configuradas com os protocolos NFS e SMB são listadas. Se apenas uma

VM de storage configurada com os protocolos NFS e SMB estiver disponível, o campo **Storage VM** não será exibido.

c. Clique em **mais Opções** e selecione **Exportar via NFS**.

A configuração padrão concede acesso total a todos os usuários. Você pode adicionar regras mais restritivas à política de exportação mais tarde.

d. Selecione **compartilhar via SMB/CIFS**.

O compartilhamento é criado com uma lista de controle de acesso (ACL) padrão definida como "Controle total" para o grupo **todos**. Você pode adicionar restrições à ACL mais tarde.

e. Se você clicar em **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.

Como alternativa, você pode continuar a ativar quaisquer serviços adicionais necessários, como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.

2. em um cliente Linux, verifique se a exportação está acessível.
   a. Crie e monte o volume usando a interface de rede da VM de armazenamento.
   b. No volume recém-montado, crie um arquivo de teste, escreva texto nele e exclua o arquivo.
3. Em um cliente Windows, faça o seguinte para verificar se o compartilhamento está acessível.
   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\_SMB_Server_Name__Share_Name_`
   b. Na unidade recém-criada, crie um arquivo de teste, escreva texto para ele e exclua o arquivo.

Depois de verificar o acesso, você pode "Restrinja o acesso do cliente com a política de exportação do volume, restrinja o acesso do cliente com a ACL de compartilhamento"e definir qualquer propriedade e permissões desejadas no volume exportado e compartilhado.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

  - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
  - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
  - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado,

poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**) no qual deseja colocar o volume que está criando.

Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.

- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

  Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.

- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne Etapa 2 no fluxo de trabalhoao provisionamento multiprotocolo completo para servidores Windows e Linux.

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
Gerenciador de sistema Clássico (ONTAP 9 .7 e anteriores)	"Visão geral da configuração multiprotocolo SMB e NFS"
A interface da linha de comando ONTAP	• "Visão geral da configuração SMB com a CLI" • "Visão geral da configuração de NFS com a CLI" • "Quais são os estilos de segurança e seus efeitos" • "Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo"

Acesso de cliente seguro com Kerberos

Ative o Kerberos para proteger o acesso ao armazenamento para clientes nas.

Este procedimento configura o Kerberos em uma VM de armazenamento existente habilitada "NFS"para ou "SMB".

Antes de começar, você deve ter configurado DNS, NTP e "LDAP"no sistema de armazenamento.

Passos

1. Na linha de comando ONTAP, defina permissões UNIX para o volume raiz da VM de armazenamento.

   a. Exiba as permissões relevantes no volume raiz da VM de armazenamento: `volume show -volume root_vol_name-fields user,group,unix-permissions`

O volume raiz da VM de storage deve ter a seguinte configuração:

Nome…	A definir…
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	755

a. Se esses valores não forem exibidos, use o `volume modify` comando para atualizá-los.

2. Definir permissões de usuário para o volume raiz da VM de armazenamento.

a. Exibir os usuários locais do UNIX: `vserver services name-service unix-user show -vserver vserver_name`

A VM de storage deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal
nfs	500	0
raiz	0	0

+
Nota: o usuário NFS não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS; consulte a etapa 5.

a. Se esses valores não forem exibidos, use o `vserver services name-service unix-user modify` comando para atualizá-los.

3. Definir permissões de grupo para o volume raiz da VM de armazenamento.

a. Exibir os grupos UNIX locais: `vserver services name-service unix-group show -vserver vserver_name`

A VM de armazenamento deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0

a. Se esses valores não forem exibidos, use o `vserver services name-service unix-group modify` comando para atualizá-los.

4. Mude para o System Manager para configurar o Kerberos
5. No System Manager, clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
6. Clique em **Configurações**.
7. Clique → em Kerberos.
8. Clique em **Add** em Kerberos Realm e complete as seguintes seções:
   - Adicione o realm Kerberos

Insira os detalhes de configuração dependendo do fornecedor do KDC.

- Adicionar interface de rede ao realm

  Clique em **Add** e selecione uma interface de rede.

9. Se desejado, adicione mapeamentos de nomes principais do Kerberos aos nomes de usuário locais.
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Clique em **Configurações** e, em seguida, clique em **Mapeamento de nomes**.
   c. Em **Kerberos para UNIX**, adicione padrões e substituições usando expressões regulares.

Ative ou desative o acesso seguro do cliente NFS com TLS

Você pode melhorar a segurança das conexões NFS configurando o NFS em TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS. Você pode configurá-lo em uma VM de armazenamento existente habilitada para "NFS"o .

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

"requisitos"Consulte o para NFS sobre TLS.

1. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
2. No bloco **NFS**, clique em **NFS over TLS settings**.
3. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja ativar o TLS.
4. Clique em ⋮ para essa interface.
5. Clique em **Ativar**.
6. Na caixa de diálogo **Configuração TLS da interface de rede**, inclua um certificado para uso com TLS selecionando uma das seguintes opções:
   - **Certificado instalado**: Escolha um certificado previamente instalado na lista suspensa.
   - **Novo certificado**: Escolha um nome comum para o certificado.
   - **Certificado assinado por CA externo**: Siga as instruções para colar o conteúdo do seu certificado e chave privada nas caixas.
7. Clique em **Salvar**.

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

Passos

1. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
2. No bloco **NFS**, clique em **NFS over TLS settings**.
3. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja desativar TLS.
4. Clique em ⋮ para essa interface.
5. Clique em **Desativar**.
6. Na caixa de diálogo de confirmação resultante, selecione **Disable**.

Fornecer acesso ao cliente com serviços de nome

Ative o ONTAP para procurar informações de host, usuário, grupo ou netgroup usando LDAP ou NIS para autenticar clientes nas.

Este procedimento cria ou modifica configurações LDAP ou NIS em uma VM de armazenamento existente habilitada para "NFS" ou "SMB".

Para configurações LDAP, você deve ter os detalhes de configuração LDAP necessários em seu ambiente e você deve usar um esquema LDAP padrão do ONTAP.

Passos

1. Configure o serviço necessário: Clique em **Storage > Storage VMs**.
2. Selecione a VM de armazenamento, clique em **Definições** e, em seguida, clique ⚙ em para LDAP ou NIS.
3. Inclua quaisquer alterações no switch de serviços de nome: Clique ✎ em Name Services Switch.

Gerencie diretórios e arquivos

Expanda a exibição do volume do System Manager para exibir e excluir diretórios e arquivos.

A partir do ONTAP 9.9,1, os diretórios são excluídos com a funcionalidade de exclusão assíncrona de diretório de baixa latência.

Para obter mais informações sobre como visualizar sistemas de arquivos no ONTAP 9.9,1 e posterior, "Visão geral do File System Analytics"consulte .

Passo

1. Selecione **armazenamento > volumes**. Expanda um volume para ver o seu conteúdo.

Gerencie usuários e grupos específicos do host com o System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para gerenciar usuários e grupos específicos de um host UNIX ou Windows.

Você pode executar os seguintes procedimentos:

Windows	UNIX

• Exibir usuários e grupos do Windows • [add-edit-delete-Windows] • [manage-windows-users]	• Exibir usuários e grupos UNIX • [add-edit-delete-UNIX] • [manage-unix-users]

Exibir usuários e grupos do Windows

No System Manager, você pode exibir uma lista de usuários e grupos do Windows.

Passos

1. No System Manager, clique em **Storage > Storage VMs**.
2. Selecione a VM de armazenamento e, em seguida, selecione a guia **Configurações**.
3. Role até a área **Host Users and Groups**.

   A seção **Windows** exibe um resumo do número de usuários em cada grupo associado à VM de armazenamento selecionada.

4. Clique → na seção **Windows**.
5. Clique na guia **Groups** e, em seguida, clique ⌄ ao lado de um nome de grupo para exibir detalhes sobre esse grupo.
6. Para exibir os usuários em um grupo, selecione o grupo e clique na guia **usuários**.

Adicione, edite ou exclua um grupo do Windows

No System Manager, você pode gerenciar grupos do Windows adicionando, editando ou excluindo-os.

Passos

1. No System Manager, veja a lista de grupos do Windows. Exibir usuários e grupos do WindowsConsulte a .
2. Na guia **Groups**, você pode gerenciar grupos com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um grupo	1. Clique + Add em . 2. Introduza as informações do grupo. 3. Especifique Privileges. 4. Especifique membros do grupo (adicione usuários locais, usuários de domínio ou grupos de domínio).
Edite um grupo	1. Ao lado do nome do grupo, clique ⋮ em e, em seguida, clique em **Editar**. 2. Modifique as informações do grupo.

Eliminar um grupo	1. Marque a caixa ao lado do grupo ou grupos que deseja excluir. 2. Clique Delete em . **Observação:** você também pode excluir um único grupo clicando ⋮ ao lado do nome do grupo e clicando em **Excluir**.

Gerenciar usuários do Windows

No System Manager, você pode gerenciar usuários do Windows adicionando, editando, excluindo, habilitando ou desativando-os. Você também pode alterar a senha de um usuário do Windows.

Passos

1. No System Manager, visualize a lista de utilizadores do grupo. Exibir usuários e grupos do WindowsConsulte a .
2. Na guia **usuários**, você pode gerenciar usuários com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um utilizador	1. Clique + Add em . 2. Introduza as informações do utilizador.
Editar um utilizador	1. Ao lado do nome de usuário, clique ⋮ em e, em seguida, clique em **Editar**. 2. Modifique as informações do usuário.
Eliminar um utilizador	1. Marque a caixa ao lado do usuário ou usuários que você deseja excluir. 2. Clique Delete em . **Observação:** você também pode excluir um único usuário clicando ⋮ ao lado do nome de usuário e clicando em **Excluir**.
Alterar a palavra-passe do utilizador	1. Ao lado do nome de usuário, clique ⋮ em e, em seguida, clique em **alterar senha**. 2. Introduza a nova palavra-passe e confirme-a.
Ativar um utilizador	1. Marque a caixa ao lado de cada usuário desativado que você deseja habilitar. 2. Clique Enable em .

Desative um usuário	1. Marque a caixa ao lado de cada usuário habilitado que você deseja desativar. 2. Clique Disable em .

Exibir usuários e grupos UNIX

No System Manager, você pode exibir uma lista de usuários e grupos UNIX.

Passos

1. No System Manager, clique em **Storage > Storage VMs**.
2. Selecione a VM de armazenamento e, em seguida, selecione a guia **Configurações**.
3. Role até a área **Host Users and Groups**.

   A seção **UNIX** exibe um resumo do número de usuários em cada grupo associado à VM de armazenamento selecionada.

4. Clique → na seção **UNIX**.
5. Clique na guia **Groups** para exibir detalhes sobre esse grupo.
6. Para exibir os usuários em um grupo, selecione o grupo e clique na guia **usuários**.

Adicione, edite ou exclua um grupo UNIX

No System Manager, você pode gerenciar grupos UNIX adicionando, editando ou excluindo-os.

Passos

1. No System Manager, veja a lista de grupos UNIX. Exibir usuários e grupos UNIXConsulte a .
2. Na guia **Groups**, você pode gerenciar grupos com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um grupo	1. Clique + Add em . 2. Introduza as informações do grupo. 3. (Opcional) Especifique usuários associados.
Edite um grupo	1. Selecione o grupo. 2. Clique Edit em . 3. Modifique as informações do grupo. 4. (Opcional) Adicionar ou remover usuários.
Eliminar um grupo	1. Selecione o grupo ou grupos que deseja excluir. 2. Clique Delete em .

Gerenciar usuários UNIX

No System Manager, você pode gerenciar usuários do Windows adicionando, editando ou excluindo-os.

Passos

1. No System Manager, visualize a lista de utilizadores do grupo. Exibir usuários e grupos UNIXConsulte a .
2. Na guia **usuários**, você pode gerenciar usuários com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um utilizador	1. Clique + Add em . 2. Introduza as informações do utilizador.
Editar um utilizador	1. Selecione o utilizador que pretende editar. 2. Clique Edit em . 3. Modifique as informações do usuário.
Eliminar um utilizador	1. Selecione o utilizador ou utilizadores que pretende eliminar. 2. Clique Delete em .

Monitorar clientes ativos NFS

A partir do ONTAP 9.8, o Gerenciador de sistema mostra quais conexões de cliente NFS estão ativas quando o NFS é licenciado em um cluster.

Isso permite verificar rapidamente quais clientes NFS estão ativamente conetados a uma VM de storage, que estão conetados, mas ociosos, e quais são desconetados.

Para cada endereço IP do cliente NFS, o visor **Clientes NFS** mostra: * Hora do último acesso * Endereço IP da interface de rede * versão da conexão NFS * Nome da VM de armazenamento

Além disso, uma lista de clientes NFS ativos nas últimas 48 horas também é mostrada na exibição **Storage>volumes** e uma contagem de clientes NFS é incluída na exibição **Dashboard**.

Passo

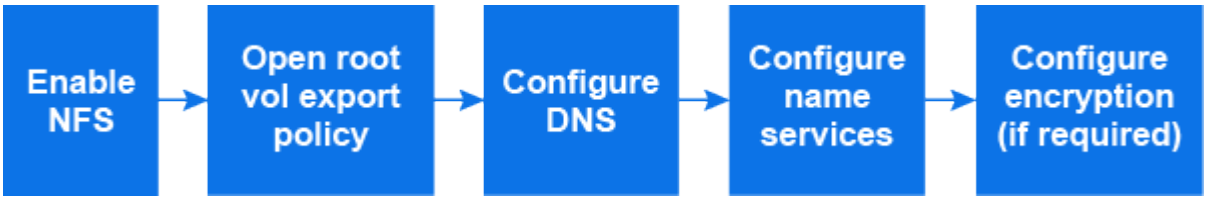
1. Exibir atividade do cliente NFS: Clique em **hosts > clientes NFS**.

Ative o armazenamento nas

Ative o storage nas para servidores Linux usando NFS

Crie ou modifique VMs de storage para habilitar servidores NFS para fornecer dados a clientes Linux.

Ative uma VM de storage nova ou existente para o protocolo NFS usando este procedimento.



Antes de começar

Certifique-se de que anotou os detalhes de configuração de qualquer rede, autenticação ou serviços de segurança necessários no seu ambiente.

Passos

1. Habilite o NFS em uma VM de storage.
   - Para novas VMs de armazenamento: Clique em **Storage > Storage VMs**, clique em **Add**, insira um nome de VM de armazenamento e, na guia **SMB/CIFS, NFS, S3**, selecione **Enable NFS**.
     i. Confirme o idioma predefinido.
     ii. Adicione interfaces de rede.
     iii. Atualizar as informações da conta do administrador da VM de armazenamento (opcional).
   - Para VMs de armazenamento existentes: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento, clique em **Settings** e, em seguida, clique em **NFS**.
2. Abra a política de exportação do volume raiz da VM de storage:
   a. Clique em **Storage > volumes**, selecione o volume raiz da VM de armazenamento (que por padrão é *volume-name* _root) e, em seguida, clique na política exibida em **Export Policy**.
   b. Clique em **Add** para adicionar uma regra.
      - Especificação do cliente `0.0.0.0/0`
      - Protocolos de acesso: NFS
      - Detalhes de acesso: UNIX Read-only
3. Configurar DNS para resolução de nome de host: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento, clique em **Configurações** e, em seguida, clique em **DNS**.
4. Configure os serviços de nomes conforme necessário.
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e clique em for LDAP ou NIS.
   b. Clique no mosaico Name Services Switch para incluir quaisquer alterações.
5. Configure a encriptação, se necessário:

Configurar TLS para clientes NFS

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Passos

1. Consulte "requisitos"o para NFS sobre TLS antes de começar.
2. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
3. No bloco **NFS**, clique em **NFS over TLS settings**.
4. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja ativar o TLS.
5. Clique em ⋮ para essa interface.
6. Clique em **Ativar**.
7. Na caixa de diálogo **Configuração TLS da interface de rede**, inclua um certificado para uso com TLS selecionando uma das seguintes opções:
   - **Certificado instalado**: Escolha um certificado previamente instalado na lista suspensa.
   - **Novo certificado**: Escolha um nome comum para o certificado.
   - **Certificado assinado por CA externo**: Siga as instruções para colar o conteúdo do seu certificado e chave privada nas caixas.
8. Clique em **Salvar**.

Configurar Kerberos

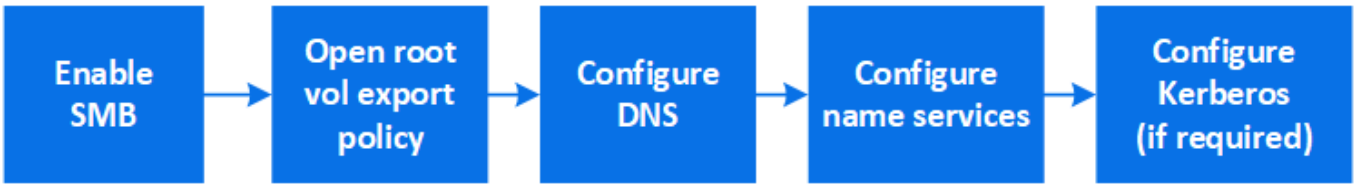
Passos

1. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
2. Clique →no mosaico Kerberos e, em seguida, clique em **Add**.

Ative o armazenamento nas para servidores Windows usando SMB

Crie ou modifique VMs de storage para habilitar servidores SMB para fornecer dados aos clientes Windows.

Este procedimento permite uma VM de storage nova ou existente para o protocolo SMB. Supõe-se que os detalhes de configuração estejam disponíveis para qualquer rede, autenticação ou serviços de segurança necessários em seu ambiente.



Passos

1. Habilite o SMB em uma VM de storage.
   a. Para novas VMs de armazenamento: Clique em **Storage > Storage VMs**, clique em **Add**, insira um nome de VM de armazenamento e, na guia **SMB/CIFS, NFS, S3**, selecione **Enable SMB/CIFS**.

- Introduza as seguintes informações:
  - Nome e senha do administrador
  - Nome do servidor
  - Domínio do diretório ativo
- Confirme a unidade organizacional.
- Confirme os valores DNS.
- Confirme o idioma predefinido.
- Adicione interfaces de rede.
- Atualizar as informações da conta do administrador da VM de armazenamento (opcional).

b. Para VMs de armazenamento existentes:: Clique em **armazenamento > armazenamento de VMs**, selecione uma VM de armazenamento, clique em **Configurações** e, em seguida, clique em **SMB**.

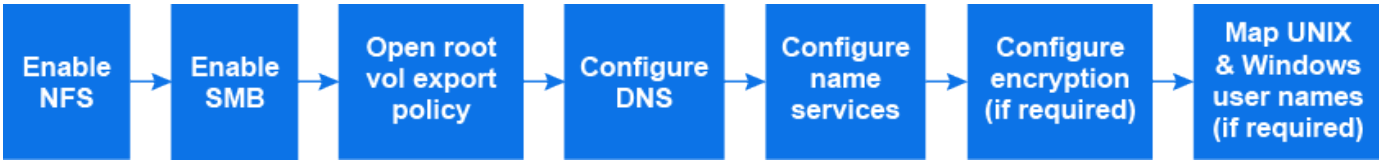
2. Abra a política de exportação do volume raiz da VM de storage:
   a. Clique em **Storage > volumes**, selecione o volume raiz da VM de armazenamento (que por padrão é *volume-name_root*) e clique na política exibida em **Export Policy**.
   b. Clique em **Add** para adicionar uma regra.
      - Especificação do cliente `0.0.0.0/0`
      - Protocolos de acesso: SMB
      - Detalhes de acesso: NTFS somente leitura
3. Configurar DNS para resolução de nome de host:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e, em seguida, clique em **DNS**.
   b. Mude para o servidor DNS e mapeie o servidor SMB.
      - Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP da interface de rede de dados.
      - Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico de alias (CNAME resource record) para mapear cada alias para o endereço IP da interface de rede de dados do servidor SMB.
4. Configure os serviços de nomes conforme necessário
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e clique em **LDAP** ou **NIS**.
   b. Inclua quaisquer alterações no arquivo de switch de serviços de nome: Clique em **Name Services Switch**.
5. Configure Kerberos se necessário:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
   b. Clique em **Kerberos** e, em seguida, clique em **Add**.

Habilite o storage nas para Windows e Linux usando NFS e SMB

Crie ou modifique VMs de storage para permitir que os servidores NFS e SMB forneçam dados a clientes Linux e Windows.

Habilite uma VM de storage nova ou existente para atender aos protocolos NFS e SMB usando este

procedimento.



Antes de começar

Certifique-se de que anotou os detalhes de configuração de qualquer rede, autenticação ou serviços de segurança necessários no seu ambiente.

Passos

1. Habilite NFS e SMB em uma VM de storage.
   a. Para novas VMs de armazenamento: Clique em **Storage > Storage VMs**, clique em **Add**, insira um nome de VM de armazenamento e, na guia **SMB/CIFS, NFS, S3**, selecione **Enable SMB/CIFS** e **Enable NFS**.
   b. Introduza as seguintes informações:
      - Nome e senha do administrador
      - Nome do servidor
      - Domínio do diretório ativo
   c. Confirme a unidade organizacional.
   d. Confirme os valores DNS.
   e. Confirme o idioma predefinido.
   f. Adicione interfaces de rede.
   g. Atualizar as informações da conta do administrador da VM de armazenamento (opcional).
   h. Para VMs de armazenamento existentes: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento e clique em **Settings**. Conclua as subetapas a seguir se NFS ou SMB ainda não estiver habilitado.
      - Clique em **NFS**.
      - Clique em **SMB**.
2. Abra a política de exportação do volume raiz da VM de storage:
   a. Clique em **Storage > volumes**, selecione o volume raiz da VM de armazenamento (que por padrão é *volume-name_root*) e clique na política exibida em **Export Policy**.
   b. Clique em **Add** para adicionar uma regra.
      - Especificação do cliente `0.0.0.0/0`
      - Protocolos de acesso: NFS
      - Detalhes de acesso: Somente leitura NFS
3. Configurar DNS para resolução de nome de host:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e, em seguida, clique em **DNS**.
   b. Quando a configuração DNS estiver concluída, mude para o servidor DNS e mapeie o servidor SMB.
      - Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP da interface de rede de dados.

- Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico de alias (CNAME resource record) para mapear cada alias para o endereço IP da interface de rede de dados do servidor SMB.

4. Configure os serviços de nomes conforme necessário:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e clique em for LDAP ou NIS.
   b. Inclua quaisquer alterações no arquivo de switch de serviços de nome: Clique em **Name Services Switch**.
5. Configure a autenticação e a criptografia, se necessário:

Configurar TLS para clientes NFS

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Passos

a. Consulte "requisitos"o para NFS sobre TLS antes de começar.
b. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
c. No bloco **NFS**, clique em **NFS over TLS settings**.
d. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja ativar o TLS.
e. Clique em para essa interface.
f. Clique em **Ativar**.
g. Na caixa de diálogo **Configuração TLS da interface de rede**, inclua um certificado para uso com TLS selecionando uma das seguintes opções:
   - **Certificado instalado**: Escolha um certificado previamente instalado na lista suspensa.
   - **Novo certificado**: Escolha um nome comum para o certificado.
   - **Certificado assinado por CA externo**: Siga as instruções para colar o conteúdo do seu certificado e chave privada nas caixas.
h. Clique em **Salvar**.

Configurar Kerberos

Passos

a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
b. Clique no mosaico Kerberos e, em seguida, clique em **Add**.

6. Mapeie nomes de usuário UNIX e Windows, se necessário: Clique em **Mapeamento de nomes** e clique em **Adicionar**.

   Você deve fazer isso somente se o seu site tiver contas de usuário do Windows e UNIX que não mapeem implicitamente, ou seja, quando a versão minúscula de cada nome de usuário do Windows corresponder ao nome de usuário do UNIX. Você pode mapear nomes de usuários usando LDAP, NIS ou usuários locais. Se você tiver dois conjuntos de usuários que não correspondem, você deve configurar o mapeamento de nomes.

Configurar o NFS com a CLI

Visão geral da configuração de NFS com a CLI

Você pode usar os comandos de CLI do ONTAP 9 para configurar o acesso de cliente NFS a arquivos contidos em um novo volume ou qtree em uma máquina virtual de storage (SVM) nova ou existente.

Utilize estes procedimentos se pretender configurar o acesso a um volume ou qtree da seguinte forma:

- Você deseja usar qualquer versão do NFS atualmente compatível com ONTAP: NFSv3, NFSv4, NFSv4,1, NFSv4,2 ou NFSv4,1 com pNFS.
- Você deseja usar a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

  Para usar o System Manager para configurar o acesso multiprotocolo nas, "Provisionar storage nas para Windows e Linux usando NFS e SMB"consulte .

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.

  Detalhes sobre a sintaxe de comando estão disponíveis nas páginas de ajuda CLI e man do ONTAP.

- As permissões de arquivo UNIX serão usadas para proteger o novo volume.
- Você tem o administrador de clusters Privileges, e não o Privileges do administrador da SVM.

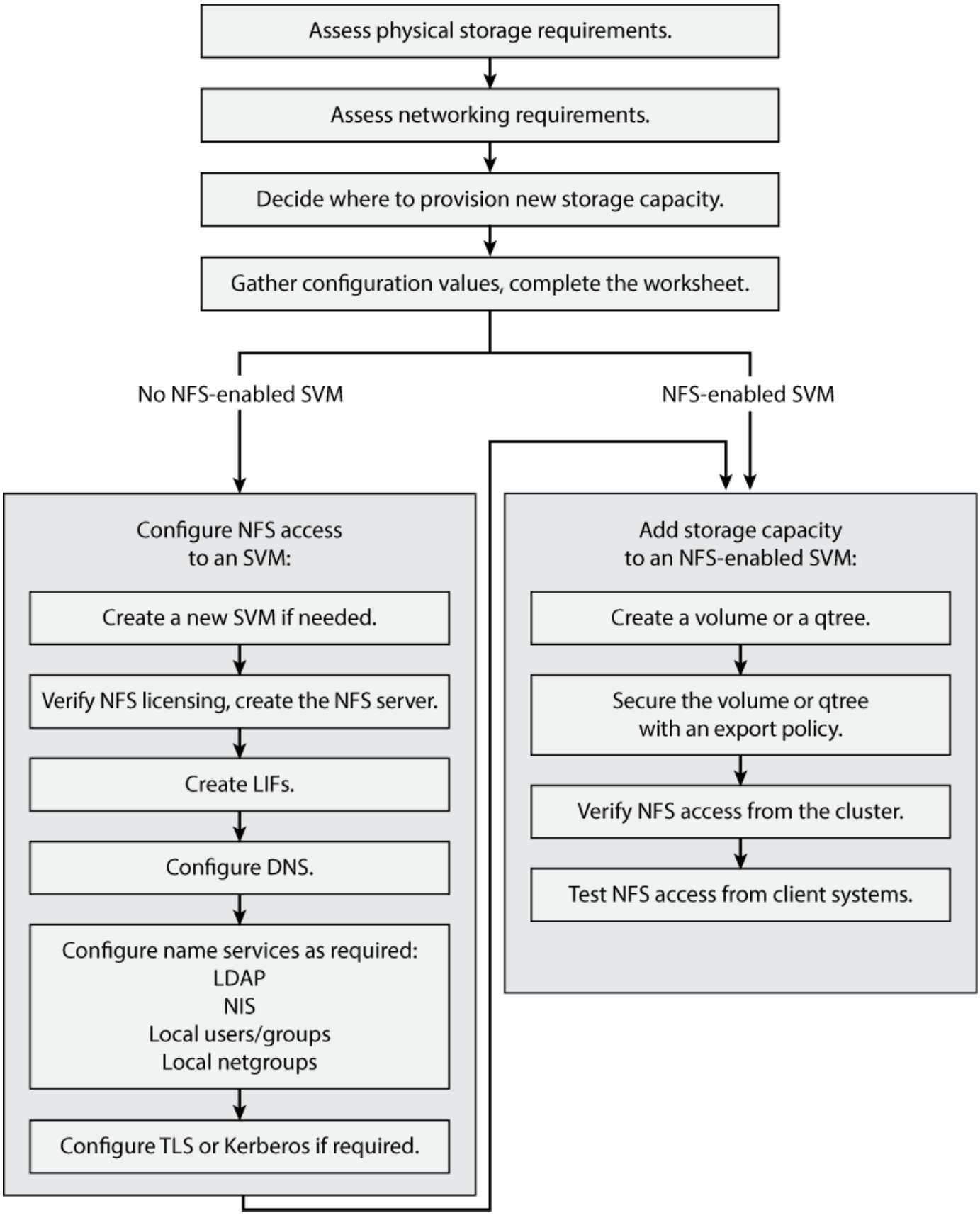
Se quiser obter detalhes sobre a gama de capacidades do protocolo NFS da ONTAP, consulte o "Visão geral de referência de NFS".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Consulte…
O Gerenciador de sistema redesenhado (disponível com o ONTAP 9.7 e posterior)	"Provisione storage nas para servidores Linux usando NFS"
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores	"Visão geral da configuração NFS"

Fluxo de trabalho de configuração NFS

A configuração do NFS envolve a avaliação dos requisitos de rede e storage físico e, depois, a escolha de um fluxo de trabalho específico para sua meta: Configurar o acesso NFS a uma nova SVM ou existente, ou adicionar um volume ou qtree a uma SVM existente que já esteja totalmente configurada para acesso ao NFS.


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

Preparação

Avaliar os requisitos de armazenamento físico

Antes de provisionar o storage NFS para clientes, você deve garantir que haja espaço suficiente em um agregado existente para o novo volume. Se não houver, você poderá adicionar discos a um agregado existente ou criar um novo agregado do tipo desejado.

Passos

1. Exibir espaço disponível em agregados existentes:

   ```
   storage aggregate show
   ```

   Se houver um agregado com espaço suficiente, Registre seu nome na Planilha.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. Se não houver agregados com espaço suficiente, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede

Antes de fornecer storage NFS aos clientes, verifique se a rede está configurada corretamente para atender aos requisitos de provisionamento de NFS.

O que você vai precisar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)

- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Passos

1. Exiba as portas físicas e virtuais disponíveis:

   `network port show`

   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.
   - Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis

   `network subnet show`

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis:

   `network ipspace show`

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster:

   `network options ipv6 show`

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decidir onde provisionar nova capacidade de storage NFS

Antes de criar um novo volume ou qtree NFS, você precisa decidir se deseja colocá-lo em uma SVM nova ou existente e quanto de configuração o SVM precisa. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um volume ou qtree em um novo SVM ou em um SVM existente que tenha o NFS habilitado, mas não configurado, siga as etapas em "Configurar acesso NFS a um SVM" e "Adicionar storage NFS a um SVM habilitado para NFS".

  Configurar o acesso NFS a uma SVM

  Adicionar storage NFS a uma SVM habilitada para NFS

  Você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

  - Você está habilitando o NFS em um cluster pela primeira vez.
  - Você tem SVMs existentes em um cluster no qual não deseja habilitar o suporte a NFS.

- Você tem um ou mais SVMs habilitados para NFS em um cluster e deseja outro servidor NFS em um namespace isolado (cenário de alocação a vários clientes). Você também deve escolher essa opção para provisionar storage em uma SVM existente que tenha o NFS habilitado, mas não configurado. Esse pode ser o caso se você criou o SVM para acesso à SAN ou se nenhum protocolo foi habilitado quando o SVM foi criado.

Depois de ativar o NFS no SVM, proceda ao provisionamento de um volume ou qtree.

- Se você quiser provisionar um volume ou qtree em uma SVM atual totalmente configurada para acesso NFS, siga as etapas em "adicionando storage NFS a uma SVM habilitado para NFS".

  Adição de storage NFS a uma SVM habilitada para NFS

Planilha para coletar informações de configuração de NFS

A Planilha de configuração NFS permite coletar as informações necessárias para configurar o acesso NFS para clientes.

Você deve completar uma ou ambas as seções da Planilha, dependendo da decisão tomada sobre onde provisionar o armazenamento:

Se você estiver configurando o acesso NFS a uma SVM, deve concluir ambas as seções.

- Configurando o acesso NFS a uma SVM
- Adição de capacidade de storage a um SVM habilitado para NFS

Se você estiver adicionando capacidade de storage a um SVM habilitado para NFS, deverá concluir apenas:

- Adição de capacidade de storage a um SVM habilitado para NFS

Configurar o acesso NFS a uma SVM

Parâmetros para criar um SVM

Você fornece esses valores com o `vserver create` comando se estiver criando um novo SVM.

Campo	Descrição	O seu valor
`-vserver`	Nome fornecido para o novo SVM que é um nome de domínio totalmente qualificado (FQDN) ou que segue outra convenção que impõe nomes exclusivos de SVM em um cluster.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para uma nova capacidade de storage NFS.	
`-rootvolume`	Um nome exclusivo fornecido para o volume raiz da SVM.	

`-rootvolume-security-style`	Use o estilo de segurança UNIX para SVM.	`unix`
`-language`	Use a configuração de idioma padrão neste fluxo de trabalho.	`C.UTF-8`
`ipspace`	Os IPspaces são espaços de endereço IP distintos nos quais residem (máquinas virtuais de armazenamento (SVMs)).	

Parâmetros para criar um servidor NFS

Você fornece esses valores com o `vserver nfs create` comando ao criar um novo servidor NFS e especificar versões NFS compatíveis.

Se estiver a ativar o NFSv4 ou posterior, deve utilizar o LDAP para melhorar a segurança.

Campo	Descrição	O seu valor
`-v3 -v4.0, , -v4.1, , -v4.1 -pnfs`	Habilite versões NFS conforme necessário. O v4,2 também é suportado no ONTAP 9.8 e posterior quando `v4.1` está ativado.	
`-v4-id-domain`	Nome de domínio de mapeamento de ID.	
`-v4-numeric-ids`	Suporte para IDs de proprietário numéricos (ativado ou desativado).	

Parâmetros para ativar a criptografia TLS para conexões NFS

Você fornece esses valores com o `vserver nfs tls interface enable` comando.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Campo	Descrição	O seu valor
`-vserver`	O vserver no qual a interface lógica existe.	

`-lif`	O nome da interface lógica na qual você deseja habilitar a criptografia em trânsito usando NFS sobre TLS.	
`-certificate-name`	O nome do certificado X,509 configurado na VM de armazenamento.	

Parâmetros para criar um LIF

Você fornece esses valores com o `network interface create` comando quando você está criando LIFs.

Se você estiver usando Kerberos, você deve habilitar Kerberos em várias LIFs.

Campo	Descrição	O seu valor
`-lif`	Um nome que você fornece para o novo LIF.	
`-role`	Use a função de LIF de dados neste fluxo de trabalho.	`data`
`-data-protocol`	Utilize apenas o protocolo NFS neste fluxo de trabalho.	`nfs`
`-home-node`	O nó ao qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-home-port`	A porta ou grupo de interface para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-address`	O endereço IPv4 ou IPv6 no cluster que será usado para acesso aos dados pelo novo LIF.	
`-netmask`	A máscara de rede e o gateway para o LIF.	
`-subnet`	Um conjunto de endereços IP. Usado em vez `-address` de e `-netmask` para atribuir endereços e netmasks automaticamente.	

`-firewall-policy`	Use a política de firewall de dados padrão neste fluxo de trabalho.	`data`

Parâmetros para resolução de nome de host DNS

Você fornece esses valores com o `vserver services name-service dns create` comando quando você está configurando o DNS.

Campo	Descrição	O seu valor
`-domains`	Até cinco nomes de domínio DNS.	
`-name-servers`	Até três endereços IP para cada servidor de nomes DNS.	

Informações do serviço de nomes

Parâmetros para criar usuários locais

Você fornece esses valores se estiver criando usuários locais usando o `vserver services name-service unix-user create` comando. Se você estiver configurando usuários locais carregando um arquivo contendo usuários UNIX de um identificador de recurso uniforme (URI), não será necessário especificar esses valores manualmente.

	Nome de utilizador (`-user`)	ID de utilizador (`-id`)	ID do grupo (`-primary-gid`)	Nome completo (`-full-name`)
Exemplo	johnm	123	100	John Miller
1				
2				
3				
…				
n				

Parâmetros para criar grupos locais

Você fornece esses valores se estiver criando grupos locais usando o `vserver services name-service unix-group create` comando. Se você estiver configurando grupos locais carregando um arquivo contendo grupos UNIX de um URI, não será necessário especificar esses valores manualmente.

	Nome do grupo (`-name`)	ID do grupo (`-id`)
Exemplo	Engenharia	100

1		
2		
3		
…		
n		

Parâmetros para NIS

Você fornece esses valores com o `vserver services name-service nis-domain create` comando.

A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

Campo	Descrição	O seu valor
`-domain`	O domínio NIS que o SVM usará para pesquisas de nomes.	
`-active`	O servidor de domínio NIS ativo.	`true` ou `false`
`-servers`	ONTAP 9.0, 9,1: Um ou mais endereços IP de servidores NIS usados pela configuração do domínio NIS.	
`-nis-servers`	ONTAP 9.2: Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores NIS usados pela configuração do domínio.	

Parâmetros para LDAP

Você fornece esses valores com o `vserver services name-service ldap client create` comando.

Você também precisará de um arquivo de certificado CA raiz autoassinado `.pem`.

A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM para o qual você deseja criar uma configuração de cliente LDAP.	
`-client-config`	O nome atribuído para a nova configuração de cliente LDAP.	
`-servers`	ONTAP 9.0, 9,1: Um ou mais servidores LDAP por endereço IP em uma lista separada por vírgulas.	
`-ldap-servers`	ONTAP 9.2: Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores LDAP.	
`-query-timeout`	Utilize os segundos predefinidos `3` para este fluxo de trabalho.	`3`
`-min-bind-level`	O nível mínimo de autenticação BIND. A predefinição é `anonymous`. Deve ser definido como `sasl` se a assinatura e a vedação estiverem configuradas.	
`-preferred-ad-servers`	Um ou mais servidores preferenciais do ative Directory por endereço IP em uma lista delimitada por vírgulas.	
`-ad-domain`	O domínio do ative Directory.	
`-schema`	O modelo de esquema a ser usado. Você pode usar um esquema padrão ou personalizado.	
`-port`	Utilize a porta de servidor LDAP predefinida `389` para este fluxo de trabalho.	`389`
`-bind-dn`	O nome distinto do usuário Bind.	
`-base-dn`	A base distinguiu o nome. O padrão é `""` (root).	

Campo	Descrição	O seu valor
`-base-scope`	Use o escopo de pesquisa base padrão `subnet` para esse fluxo de trabalho.	`subnet`
`-session-security`	Ativa a assinatura ou assinatura LDAP e a vedação. A predefinição é `none`.	
`-use-start-tls`	Ativa LDAP em TLS. A predefinição é `false`.	

Parâmetros para autenticação Kerberos

Você fornece esses valores com o `vserver nfs kerberos realm create` comando. Alguns dos valores serão diferentes dependendo se você usa o Microsoft ative Directory como um servidor KDC (Key Distribution Center), ou MIT ou outro servidor KDC UNIX.

Campo	Descrição	O seu valor
`-vserver`	O SVM que se comunicará com o KDC.	
`-realm`	O Reino Kerberos.	
`-clock-skew`	Desvio de relógio permitido entre clientes e servidores.	
`-kdc-ip`	Endereço IP KDC.	
`-kdc-port`	Número da porta KDC.	
`-adserver-name`	Apenas Microsoft KDC: Nome do servidor DE ANÚNCIOS.	
`-adserver-ip`	Apenas Microsoft KDC: Endereço IP do servidor DE ANÚNCIOS.	
`-adminserver-ip`	UNIX KDC apenas: Endereço IP do servidor de administração.	
`-adminserver-port`	UNIX KDC apenas: Número da porta do servidor de administração.	
`-passwordserver-ip`	UNIX KDC apenas: Endereço IP do servidor de senha.	

`-passwordserver-port`	UNIX KDC apenas: Porta do servidor de senha.	
`-kdc-vendor`	Fornecedor de KDC.	Clique `Microsoft` em `Other` OK
`-comment`	Quaisquer comentários desejados.	

Você fornece esses valores com o `vserver nfs kerberos interface enable` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM para o qual você deseja criar uma configuração Kerberos.	
`-lif`	O LIF de dados no qual você ativará o Kerberos. Você pode ativar o Kerberos em várias LIFs.	
`-spn`	O nome do princípio de serviço (SPN)	
`-permitted-enc-types`	Os tipos de criptografia permitidos para Kerberos sobre NFS; `aes-256` são recomendados, dependendo dos recursos do cliente.	
`-admin-username`	As credenciais do administrador do KDC para recuperar a chave secreta do SPN diretamente do KDC. É necessária uma palavra-passe	
`-keytab-uri`	O arquivo keytab do KDC que contém a chave SPN se você não tiver credenciais de administrador KDC.	
`-ou`	A unidade organizacional (ou) sob a qual a conta de servidor do Microsoft ative Directory será criada quando você ativar o Kerberos usando um realm para o Microsoft KDC.	

Parâmetros para criar políticas e regras de exportação

Você fornece esses valores com o `vserver export-policy create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM que hospedará o novo volume.	
`-policyname`	Um nome fornecido para uma nova política de exportação.	

Você fornece esses valores para cada regra com o `vserver export-policy rule create` comando.

Campo	Descrição	O seu valor
`-clientmatch`	Especificação de correspondência do cliente.	
`-ruleindex`	Posição da regra de exportação na lista de regras.	
`-protocol`	Use NFS neste fluxo de trabalho.	`nfs`
`-rorule`	Método de autenticação para acesso somente leitura.	
`-rwrule`	Método de autenticação para acesso de leitura e gravação.	
`-superuser`	Método de autenticação para acesso de superusuário.	
`-anon`	ID de usuário para o qual usuários anônimos são mapeados.	

Você deve criar uma ou mais regras para cada política de exportação.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Exemplos	0,0.0,0/0	qualquer	krb5	sistema	65534
1					
2					

3					
…					
n					

Parâmetros para criar um volume

Você fornece esses valores com o `volume create` comando se estiver criando um volume em vez de uma qtree.

Campo	Descrição	O seu valor
`-vserver`	Nome de uma SVM nova ou existente que hospedará o novo volume.	
`-volume`	Um nome descritivo exclusivo que você fornece para o novo volume.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para o novo volume NFS.	
`-size`	Um número inteiro fornecido para o tamanho do novo volume.	
`-user`	Nome ou ID do usuário que é definido como o proprietário da raiz do volume.	
`-group`	Nome ou ID do grupo definido como o proprietário da raiz do volume.	
`--security-style`	Use o estilo de segurança UNIX para este fluxo de trabalho.	`unix`
`-junction-path`	Localização sob a raiz (/) onde o novo volume deve ser montado.	
`-export-policy`	Se estiver a planear utilizar uma política de exportação existente, pode introduzir o respetivo nome quando criar o volume.	

Parâmetros para criar uma qtree

Você fornece esses valores com o `volume qtree create` comando se estiver criando uma qtree em vez de um volume.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual reside o volume que contém a qtree.	
`-volume`	O nome do volume que conterá a nova qtree.	
`-qtree`	Um nome descritivo exclusivo que você fornece para a nova qtree, 64 carateres ou menos.	
`-qtree-path`	O argumento de caminho de qtree no formato `/vol/volume_name/qtree_name\>` pode ser especificado em vez de especificar volume e qtree como argumentos separados.	
`-unix-permissions`	Opcional: As permissões UNIX para a qtree.	
`-export-policy`	Se você estiver planejando usar uma política de exportação existente, poderá inserir seu nome ao criar a qtree.	

Informações relacionadas

- "Referência do comando ONTAP"

Configurar o acesso NFS a uma SVM

Criar um SVM

Se você ainda não tiver pelo menos um SVM em um cluster para fornecer acesso a dados a clientes NFS, será necessário criá-lo.

Antes de começar

- A partir do ONTAP 9.13,1, é possível definir uma capacidade máxima para uma VM de armazenamento. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

Passos

1. Criar um SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
```

ipspace_name

- Utilize a definição UNIX para a `-rootvolume-security-style` opção.
- Utilize a opção C.UTF-8 predefinida `-language`.
- A `ipspace` definição é opcional.

2. Verifique a configuração e o status do SVM recém-criado:

`vserver show -vserver` *vserver_name*

```
`Allowed Protocols`O campo deve incluir NFS. Você pode editar esta lista
mais tarde.
```

O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no ipspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

A partir do ONTAP 9.13,1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Verifique se o protocolo NFS está habilitado no SVM

Antes de configurar e usar NFS em SVMs, você deve verificar se o protocolo está ativado.

Sobre esta tarefa

Isso geralmente é feito durante a configuração do SVM, mas se você não ativou o protocolo durante a configuração, poderá ativá-lo mais tarde usando o `vserver add-protocols` comando.

Não é possível adicionar ou remover um protocolo de um LIF depois de criado.

Você também pode desativar protocolos em SVMs usando o `vserver remove-protocols` comando.

Passos

1. Verifique quais protocolos estão atualmente ativados e desativados para o SVM:

```
vserver show -vserver vserver_name -protocols
```

Você também pode usar o `vserver show-protocols` comando para exibir os protocolos atualmente habilitados em todos os SVMs no cluster.

2. Se necessário, ative ou desative um protocolo:
   - Para ativar o protocolo NFS
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - Para desativar um protocolo
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Confirme se os protocolos ativados e desativados foram atualizados corretamente:

```
vserver show -vserver vserver_name -protocols
```

Exemplo

O comando a seguir exibe quais protocolos estão atualmente ativados e desativados (permitidos e não permitidos) no SVM chamado VS1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

O comando a seguir permite o acesso por NFS adicionando `nfs` à lista de protocolos habilitados no SVM chamado VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Abra a política de exportação do volume raiz da SVM

A política de exportação padrão do volume raiz da SVM deve incluir uma regra para permitir que todos os clientes tenham acesso aberto por meio do NFS. Sem essa regra, todos os clientes NFS têm acesso negado ao SVM e seus volumes.

Sobre esta tarefa

Quando um novo SVM é criado, uma política de exportação padrão (chamada padrão) é criada automaticamente para o volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM.

Você deve verificar se o acesso está aberto a todos os clientes NFS na política de exportação padrão e, mais tarde, restringir o acesso a volumes individuais criando políticas de exportação personalizadas para volumes individuais ou qtrees.

Passos

1. Se você estiver usando uma SVM existente, verifique a política de exportação de volume raiz padrão:

```
vserver export-policy rule show
```

A saída do comando deve ser semelhante ao seguinte:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Se existir uma regra que permita o acesso aberto, esta tarefa está concluída. Caso contrário, avance para o passo seguinte.

2. Crie uma regra de exportação para o volume raiz da SVM:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Se o SVM contiver apenas volumes protegidos pelo Kerberos, você poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5` ou `krb5i`. Por exemplo:

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Verifique a criação de regras usando o `vserver export-policy rule show` comando.

Resultado

Qualquer cliente NFS agora pode acessar qualquer volume ou qtree criado no SVM.

Crie um servidor NFS

Depois de verificar se o NFS está licenciado no cluster, você pode usar o `vserver nfs create` comando para criar um servidor NFS no SVM e especificar as versões NFS compatíveis.

Sobre esta tarefa

O SVM pode ser configurado para dar suporte a uma ou mais versões de NFS. Se você estiver apoiando NFSv4 ou posterior:

- O nome de domínio de mapeamento de ID de usuário NFSv4 deve ser o mesmo no servidor NFSv4 e nos clientes de destino.

  Ele não precisa necessariamente ser o mesmo que um nome de domínio LDAP ou NIS, desde que o servidor NFSv4 e os clientes estejam usando o mesmo nome.

- Os clientes-alvo devem suportar a configuração de ID numérica NFSv4.
- Por motivos de segurança, você deve usar o LDAP para serviços de nome em implantações NFSv4.

Antes de começar

O SVM deve ter sido configurado para permitir o protocolo NFS.

Passos

1. Verifique se o NFS está licenciado no cluster:

   ```
   system license show -package nfs
   ```

   Se não estiver, contacte o seu representante de vendas.

2. Criar um servidor NFS:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Você pode optar por ativar qualquer combinação de versões NFS. Se você quiser dar suporte ao pNFS, habilite as `-v4.1` opções e `-v4.1-pnfs` .

   Se você ativar o v4 ou posterior, também deve ter certeza de que as seguintes opções estão definidas corretamente:

   - `-v4-id-domain`

     Este parâmetro opcional especifica a parte do domínio da forma de cadeia de carateres de nomes de usuário e grupo, conforme definido pelo protocolo NFSv4. Por padrão, o ONTAP usa o domínio NIS se um estiver definido; caso contrário, o domínio DNS será usado. Você deve fornecer um valor que corresponda ao nome de domínio usado pelos clientes de destino.

   - `-v4-numeric-ids`

     Este parâmetro opcional especifica se o suporte para identificadores de cadeia de carateres numéricos em atributos de proprietário NFSv4 está habilitado. A configuração padrão é ativada, mas você deve verificar se os clientes de destino a suportam.

   Você pode ativar recursos NFS adicionais mais tarde usando o `vserver nfs modify` comando.

3. Verifique se o NFS está em execução:

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Verifique se o NFS está configurado conforme desejado:

   ```
   vserver nfs show -vserver vserver_name
   ```

Exemplos

O comando a seguir cria um servidor NFS no SVM chamado VS1 com NFSv3 e NFSv4,0 ativados:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Os comandos a seguir verificam os valores de status e configuração do novo servidor NFS chamado VS1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                    General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                  Default Windows User: -
                   NFSv4.0 ACL Support: disabled
      NFSv4.0 Read Delegation Support: disabled
     NFSv4.0 Write Delegation Support: disabled
              NFSv4 ID Mapping Domain: my_domain.com
...
```

Crie um LIF

Um LIF é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

O que você vai precisar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.

- Se você estiver usando a autenticação Kerberos, ative o Kerberos em várias LIFs.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

A partir do ONTAP 9.4, o FC-NVMe é compatível. Se você estiver criando um LIF FC-NVMe, deve estar ciente do seguinte:

- O protocolo NVMe precisa ser compatível com o adaptador FC no qual o LIF é criado.
- O FC-NVMe pode ser o único protocolo de dados em LIFs de dados.
- Um tráfego de gerenciamento de manipulação de LIF deve ser configurado para cada máquina virtual de storage (SVM) que suporte SAN.
- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- Somente um LIF NVMe que manipula o tráfego de dados pode ser configurado por SVM

Passos

1. Criar um LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol nfs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

Opção	Descrição
ONTAP 9 .5 e anteriores	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9 1.6 e posterior	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

   - `-role`O parâmetro não é necessário ao criar um LIF usando uma política de serviço (a partir do ONTAP 9,6).
   - O `-data-protocol` parâmetro deve ser especificado quando o LIF é criado e não pode ser modificado mais tarde sem destruir e recriar o LIF de dados.

O `-data-protocol` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6).

- `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

  Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.

2. Verifique se o LIF foi criado com sucesso usando o `network interface show` comando.
3. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

4. Se você estiver usando Kerberos, repita as etapas 1 a 3 para criar LIFs adicionais.

   O Kerberos deve ser habilitado separadamente em cada um desses LIFs.

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

O comando a seguir mostra como criar um LIF de dados nas atribuído com a `default-data-files` política de serviço:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Ative DNS para resolução de nome de host

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os

nomes de host são resolvidos usando servidores DNS externos.

O que você vai precisar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

O *Network Management Guide* contém informações sobre a configuração de DNS dinâmico na SVM.

Passos

1. Habilite o DNS na SVM:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ⓘ A partir do ONTAP 9.2, o `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Exiba as configurações do domínio DNS usando o `vserver services name-service dns show` comando.

   O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

   ```
   vserver services name-service dns show
                                              Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide o status dos servidores de nomes usando o `vserver services name-service dns check` comando.

   O `vserver services name-service dns check` comando está disponível a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configurar serviços de nomes

Configure a visão geral dos serviços de nome

Dependendo da configuração do seu sistema de storage, o ONTAP precisa ser capaz de procurar informações de host, usuário, grupo ou netgroup para fornecer acesso adequado aos clientes. Você deve configurar serviços de nomes para permitir que o ONTAP acesse serviços de nomes locais ou externos para obter essas informações.

Você deve usar um serviço de nomes como NIS ou LDAP para facilitar pesquisas de nomes durante a autenticação do cliente. É melhor usar o LDAP sempre que possível para maior segurança, especialmente ao implantar o NFSv4 ou posterior. Você também deve configurar usuários e grupos locais caso os servidores de nomes externos não estejam disponíveis.

As informações do serviço de nomes devem ser mantidas sincronizadas em todas as fontes.

Configure a tabela do switch do serviço de nomes

Você deve configurar a tabela de switch de serviço de nomes corretamente para permitir que o ONTAP consulte serviços de nome locais ou externos para recuperar informações de mapeamento de host, usuário, grupo, netgroup ou nome.

O que você vai precisar

Você deve ter decidido quais serviços de nome deseja usar para o mapeamento de host, usuário, grupo, grupo de rede ou nome, conforme aplicável ao seu ambiente.

Se você planeja usar netgroups, todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

Sobre esta tarefa

Não inclua fontes de informação que não estejam a ser utilizadas. Por exemplo, se o NIS não estiver sendo usado em seu ambiente, não especifique a `-sources nis` opção.

Passos

1. Adicione as entradas necessárias à tabela do switch de serviço de nomes:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Verifique se a tabela do switch de serviço de nomes contém as entradas esperadas na ordem desejada:

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Se pretender efetuar quaisquer correções, tem de utilizar os `vserver services name-service ns-switch modify` comandos ou `vserver services name-service ns-switch delete`.

Exemplo

O exemplo a seguir cria uma nova entrada na tabela de opções de serviço de nomes para o SVM VS1 usar o arquivo netgroup local e um servidor NIS externo para procurar informações de netgroup nessa ordem:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Depois de terminar

- Você precisa configurar os serviços de nome especificados para o SVM para fornecer acesso aos dados.
- Se você excluir qualquer serviço de nomes para o SVM, também será necessário removê-lo da tabela de opções de serviços de nomes.

  O acesso do cliente ao sistema de armazenamento pode não funcionar como esperado, se você não conseguir excluir o serviço de nomes da tabela de opções do serviço de nomes.

Configurar usuários e grupos UNIX locais

Configure a visão geral de usuários e grupos UNIX locais

Você pode usar usuários e grupos UNIX locais no SVM para mapeamentos de nomes e autenticação. Você pode criar usuários e grupos UNIX manualmente ou carregar um arquivo contendo usuários ou grupos UNIX a partir de um identificador de recurso uniforme (URI).

Há um limite máximo padrão de 32.768 grupos de usuários UNIX locais e membros de grupo combinados no cluster. O administrador do cluster pode modificar este limite.

Crie um usuário local do UNIX

Você pode usar o `vserver services name-service unix-user create` comando para criar usuários UNIX locais. Um usuário UNIX local é um usuário UNIX criado no SVM como uma opção de serviços de nome UNIX para ser usado no processamento de mapeamentos de nomes.

Passo

1. Criar um usuário local UNIX:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* especifica o nome de usuário. O comprimento do nome de utilizador tem de ter 64 carateres ou menos.

   `-id` *`integer`* Especifica a ID de usuário que você atribui.

   `-primary-gid` *`integer`* Especifica o ID do grupo principal. Isso adiciona o usuário ao grupo principal. Depois de criar o usuário, você pode adicionar manualmente o usuário a qualquer grupo adicional desejado.

Exemplo

O comando a seguir cria um usuário UNIX local chamado johnm (nome completo "John Miller") no SVM chamado VS1. O usuário tem o ID 123 e o ID do grupo principal 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Carregue usuários UNIX locais a partir de um URI

Como alternativa à criação manual de usuários UNIX locais individuais em SVMs, você pode simplificar a tarefa carregando uma lista de usuários UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI(`vserver services name-service unix-user load-from-uri`)).

Passos

1. Crie um arquivo contendo a lista de usuários UNIX locais que você deseja carregar.

   O arquivo deve conter informações do usuário no formato UNIX `/etc/passwd`:

   `user_name: password: user_ID: group_ID: full_name`

   O comando descarta o valor *`password`* do campo e os valores dos campos após o *`full_name`* campo (*`home_directory`* e *`shell`*).

   O tamanho máximo de ficheiro suportado é de 2,5 MB.

2. Verifique se a lista não contém informações duplicadas.

   Se a lista contiver entradas duplicadas, o carregamento da lista falhará com uma mensagem de erro.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de usuários UNIX locais em SVMs a partir do URI:

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false` `especifica se pretende substituir as entradas. A predefinição é` `false`.

Exemplo

O comando a seguir carrega uma lista de usuários UNIX locais do URI `ftp://ftp.example.com/passwd` para o SVM chamado VS1. Os usuários existentes no SVM não são sobrescritos pelas informações do URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Crie um grupo UNIX local

Você pode usar o `vserver services name-service unix-group create` comando para criar grupos UNIX locais para o SVM. Grupos UNIX locais são usados com usuários UNIX locais.

Passo

1. Criar um grupo UNIX local:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* especifica o nome do grupo. O comprimento do nome do grupo deve ter 64 carateres ou menos.

   `-id` *`integer`* Especifica o ID do grupo que você atribui.

Exemplo

O comando a seguir cria um grupo local chamado eng no SVM chamado VS1. O grupo tem o ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Adicione um usuário a um grupo UNIX local

Você pode usar o `vserver services name-service unix-group adduser` comando para adicionar um usuário a um grupo UNIX suplementar que seja local para o SVM.

Passo

1. Adicionar um usuário a um grupo UNIX local:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Especifica o nome do grupo UNIX ao qual o usuário será adicionado, além do grupo principal do usuário.

Exemplo

O comando a seguir adiciona um usuário chamado Max a um grupo UNIX local chamado eng no SVM chamado VS1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Carregue grupos UNIX locais a partir de um URI

Como alternativa à criação manual de grupos UNIX locais individuais, você pode carregar uma lista de grupos UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI) usando o `vserver services name-service unix-group load-from-uri` comando.

Passos

1. Crie um arquivo contendo a lista de grupos UNIX locais que você deseja carregar.

   O arquivo deve conter informações de grupo no formato UNIX `/etc/group`:

   `group_name: password: group_ID: comma_separated_list_of_users`

   O comando descarta o valor *`password`* do campo.

   O tamanho máximo de ficheiro suportado é de 1 MB.

   O comprimento máximo de cada linha no arquivo de grupo é de 32.768 carateres.

2. Verifique se a lista não contém informações duplicadas.

A lista não deve conter entradas duplicadas, ou então carregar a lista falha. Se já houver entradas presentes no SVM, você deve definir o `-overwrite` parâmetro para `true` substituir todas as entradas existentes pelo novo arquivo ou garantir que o novo arquivo não contenha entradas que dupliquem entradas existentes.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de grupos UNIX locais no SVM a partir do URI:

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`especifica se pretende substituir as entradas. A predefinição é `false`. Se você especificar esse parâmetro como `true`, o ONTAP substituirá todo o banco de dados de grupo UNIX local existente do SVM especificado pelas entradas do arquivo que você está carregando.

Exemplo

O comando a seguir carrega uma lista de grupos UNIX locais do URI `ftp://ftp.example.com/group` para o SVM chamado VS1. Os grupos existentes no SVM não são sobrescritos pelas informações do URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Trabalhar com netgroups

Trabalhando com netgroups visão geral

Você pode usar netgroups para autenticação de usuário e para corresponder clientes em regras de política de exportação. Você pode fornecer acesso a netgroups de servidores de nomes externos (LDAP ou NIS) ou pode carregar netgroups de um identificador de recurso uniforme (URI) em SVMs usando o `vserver services name-service netgroup load` comando.

O que você vai precisar

Antes de trabalhar com netgroups, você deve garantir que as seguintes condições sejam atendidas:

- Todos os hosts em netgroups, independentemente da origem (NIS, LDAP ou arquivos locais), devem ter Registros DNS de encaminhamento (A) e reverso (PTR) para fornecer pesquisas de DNS consistentes de encaminhamento e reversão.

  Além disso, se um endereço IP de um cliente tiver vários Registros PTR, todos esses nomes de host devem ser membros do netgroup e ter Registros correspondentes A.

- Os nomes de todos os hosts em netgroups, independentemente de sua origem (NIS, LDAP ou arquivos locais), devem ser corretamente escritos e usar o caso correto. As inconsistências em nomes de host usados em netgroups podem levar a um comportamento inesperado, como verificações de exportação com falha.
- Todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

  Por exemplo, 2011:hu9:0:0:0:0:3:1 tem de ser encurtado para 2011:hu9::3:1.

Sobre esta tarefa

Quando você trabalha com netgroups, você pode executar as seguintes operações:

- Você pode usar o `vserver export-policy netgroup check-membership` comando para ajudar a determinar se um IP de cliente é membro de um determinado netgroup.
- Você pode usar o `vserver services name-service getxxbyyy netgrp` comando para verificar se um cliente faz parte de um netgroup.

  O serviço subjacente para fazer a pesquisa é selecionado com base na ordem configurada do switch do serviço de nomes.

Carregue netgroups em SVMs

Um dos métodos que você pode usar para combinar clientes em regras de política de exportação é usando hosts listados em netgroups. Você pode carregar netgroups de um URI (identificador de recurso uniforme) em SVMs como uma alternativa ao uso de netgroups armazenados em servidores de nomes externos (`vserver services name-service netgroup load`).

O que você vai precisar

Os arquivos netgroup devem atender aos seguintes requisitos antes de serem carregados em um SVM:

- O arquivo deve usar o mesmo formato de arquivo de texto netgroup apropriado que é usado para preencher NIS.

  O ONTAP verifica o formato do arquivo de texto do netgroup antes de carregá-lo. Se o arquivo contiver erros, ele não será carregado e uma mensagem será exibida indicando as correções que você tem que executar no arquivo. Depois de corrigir os erros, você pode recarregar o arquivo netgroup no SVM especificado.

- Todos os carateres alfabéticos nos nomes de host no arquivo netgroup devem estar em minúsculas.
- O tamanho máximo de ficheiro suportado é de 5 MB.
- O nível máximo suportado para netgroups de aninhamento é 1000.
- Somente nomes de host DNS primários podem ser usados ao definir nomes de host no arquivo netgroup.

  Para evitar problemas de acesso à exportação, os nomes de host não devem ser definidos usando Registros DNS CNAME ou round robin.

- As partes de usuário e domínio de triplos no arquivo netgroup devem ser mantidas vazias porque o ONTAP não as suporta.

Apenas a parte host/IP é suportada.

Sobre esta tarefa

O ONTAP suporta pesquisas netgroup-by-host para o arquivo netgroup local. Depois de carregar o arquivo netgroup, o ONTAP cria automaticamente um mapa netgroup.byhost para ativar as pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas de netgroup locais ao processar regras de política de exportação para avaliar o acesso do cliente.

Passo

1. Carregue netgroups em SVMs a partir de um URI:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Carregar o arquivo netgroup e construir o mapa netgroup.byhost pode levar vários minutos.

   Se quiser atualizar os netgroups, você pode editar o arquivo e carregar o arquivo netgroup atualizado no SVM.

Exemplo

O comando a seguir carrega definições de netgroup no SVM chamado VS1 a partir do URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verifique o status das definições do netgroup

Depois de carregar netgroups no SVM, você pode usar o `vserver services name-service netgroup status` comando para verificar o status das definições do netgroup. Isso permite determinar se as definições de netgroup são consistentes em todos os nós que fazem backup do SVM.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Verifique o status das definições do netgroup:

   `vserver services name-service netgroup status`

   Pode apresentar informações adicionais numa vista mais detalhada.

3. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Exemplo

Depois que o nível de privilégio é definido, o seguinte comando exibe o status do netgroup para todos os SVMs:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Crie uma configuração de domínio NIS

Se um NIS (Network Information Service) for usado em seu ambiente para serviços de nome, você deverá criar uma configuração de domínio NIS para o SVM usando o `vserver services name-service nis-domain create` comando.

Antes de começar

Todos os servidores NIS configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.

Se você pretende usar NIS para pesquisas de diretório, os mapas em seus servidores NIS não podem ter mais de 1.024 carateres para cada entrada. Não especifique o servidor NIS que não está em conformidade com este limite. Caso contrário, o acesso do cliente dependente de entradas NIS pode falhar.

Sobre esta tarefa

Se o seu banco de dados NIS contiver um `netgroup.byhost` mapa, o ONTAP poderá usá-lo para pesquisas mais rápidas. Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente. A partir do ONTAP 9.7, as entradas do NIS `netgroup.byhost` podem ser armazenadas em cache usando os `vserver services name-service nis-domain netgroup-database` comandos.

O uso do NIS para resolução de nome de host não é suportado.

Passos

1. Criar uma configuração de domínio NIS:

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Pode especificar até 10 servidores NIS.

   > A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

2. Verifique se o domínio foi criado:

   ```
   vserver services name-service nis-domain show
   ```

Exemplo

O comando a seguir cria uma configuração de domínio NIS para um domínio NIS chamado `nisdomain` no SVM nomeado `vs1` com um servidor NIS em endereço IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Utilize LDAP

Visão geral do uso do LDAP

Se o LDAP for usado no ambiente para serviços de nomes, você precisará trabalhar com o administrador LDAP para determinar os requisitos e as configurações do sistema de storage apropriadas e, em seguida, ativar o SVM como cliente LDAP.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores de nomes, use o `-try-channel -binding` parâmetro com o `ldap client modify` comando.

Para obter mais informações, "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows"consulte .

- Antes de configurar o LDAP para ONTAP, você deve verificar se a implantação do site atende às práticas recomendadas para configuração do servidor LDAP e do cliente. Em especial, devem ser satisfeitas as seguintes condições:
  - O nome de domínio do servidor LDAP deve corresponder à entrada no cliente LDAP.
  - Os tipos de hash de senha do usuário LDAP suportados pelo servidor LDAP devem incluir aqueles suportados pelo ONTAP:
    - CRYPT (todos os tipos) e SHA-1 (SHA, SSHA).
    - A partir do ONTAP 9.8, hashes SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 e SSHA-512) também são suportados.

- Se o servidor LDAP exigir medidas de segurança de sessão, você deve configurá-las no cliente LDAP.

  As seguintes opções de segurança de sessão estão disponíveis:

  - Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
  - INICIE O TLS
  - LDAPS (LDAP sobre TLS ou SSL)
- Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
  - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
  - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
  - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
- Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
  - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
  - Se o LDAPS for usado, o servidor LDAP deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
  - Um servidor de certificados já deve estar configurado no domínio.
- Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
  - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
    - Bidirecional
    - One-way, onde o primário confia no domínio de referência
    - Pai-filho
  - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
  - As senhas de domínio devem ser as mesmas para autenticar quando --bind-as-cifs-server definido como true.

  > As configurações a seguir não são suportadas com a busca por referência LDAP.
  >
  > - Para todas as versões do ONTAP:
  >   - Clientes LDAP em um SVM admin
  > - Para o ONTAP 9.8 e versões anteriores (eles são suportados em 9.9.1 e posteriores):
  >   - Assinatura e selagem LDAP (a `-session-security` opção)
  >   - Conexões TLS criptografadas (a `-use-start-tls` opção)
  >   - Comunicações através da porta LDAPS 636 (a `-use-ldaps-for-ad-ldap` opção)

- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

  Na maioria dos casos, um dos esquemas ONTAP padrão será apropriado. No entanto, se o esquema LDAP em seu ambiente for diferente desses, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar o cliente LDAP. Consulte o administrador LDAP sobre os requisitos para o seu ambiente.

- O uso do LDAP para resolução de nome de host não é suportado.

Para mais informações

- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"
- "Instale o certificado de CA raiz autoassinado no SVM"

Crie um novo esquema de cliente LDAP

Se o esquema LDAP no ambiente for diferente dos padrões do ONTAP, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar a configuração do cliente LDAP.

Sobre esta tarefa

A maioria dos servidores LDAP pode usar os esquemas padrão fornecidos pelo ONTAP:

- MS-AD-BIS (o esquema preferido para a maioria dos servidores AD do Windows 2012 e posteriores)
- Ad-IDMU (Windows 2008, Windows 2012 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)
- RFC-2307 (SERVIDORES LDAP UNIX)

Se você precisar usar um esquema LDAP não padrão, você deve criá-lo antes de criar a configuração do cliente LDAP. Consulte o administrador LDAP antes de criar um novo esquema.

Os esquemas LDAP padrão fornecidos pelo ONTAP não podem ser modificados. Para criar um novo esquema, você cria uma cópia e modifica a cópia de acordo.

Passos

1. Exiba os modelos de esquema de cliente LDAP existentes para identificar o que deseja copiar:

   ```
   vserver services name-service ldap client schema show
   ```

2. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

3. Faça uma cópia de um esquema cliente LDAP existente:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Modifique o novo esquema e personalize-o para o seu ambiente:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Crie uma configuração de cliente LDAP

Se você quiser que o ONTAP acesse os serviços LDAP ou ative Directory externos em seu ambiente, primeiro é necessário configurar um cliente LDAP no sistema de armazenamento.

O que você vai precisar

Um dos três primeiros servidores na lista de domínios resolvidos do ative Directory deve estar ativo e fornecendo dados. Caso contrário, esta tarefa falha.

> Existem vários servidores, dos quais mais de dois servidores estão inativos a qualquer momento.

Passos

1. Consulte o administrador LDAP para determinar os valores de configuração apropriados para o `vserver services name-service ldap client create` comando:

   a. Especifique uma conexão baseada em domínio ou baseada em endereço para servidores LDAP.

      As `-ad-domain` opções e `-servers` são mutuamente exclusivas.

      - Utilize a `-ad-domain` opção para ativar a deteção de servidor LDAP no domínio do ative Directory.
        - Você pode usar a `-restrict-discovery-to-site` opção para restringir a descoberta de servidor LDAP ao site padrão CIFS para o domínio especificado. Se você usar essa opção, também precisará especificar o site padrão CIFS com `-default-site`.
      - Você pode usar a `-preferred-ad-servers` opção para especificar um ou mais servidores preferenciais do ative Directory por endereço IP em uma lista delimitada por vírgulas. Depois que o cliente é criado, você pode modificar esta lista usando o `vserver services name-service ldap client modify` comando.
      - Use a `-servers` opção para especificar um ou mais servidores LDAP (ative Directory ou UNIX) por endereço IP em uma lista delimitada por vírgulas.

        > A `-servers` opção está obsoleta no ONTAP 9.2. A partir de ONTAP 9.2, o `-ldap -servers` campo substitui o `-servers` campo. Este campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

   b. Especifique um esquema LDAP padrão ou personalizado.

      A maioria dos servidores LDAP pode usar os esquemas somente leitura padrão fornecidos pelo ONTAP. É melhor usar esses esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão (eles são somente leitura) e, em seguida, modificando a cópia.

      Esquemas predefinidos:

      - MS-AD-BIS

        Baseado em RFC-2307bis, este é o esquema LDAP preferido para a maioria das implantações padrão do Windows 2012 e LDAP posteriores.

- `AD-IDMU`

  Baseado no ative Directory Identity Management para UNIX, esse esquema é apropriado para a maioria dos servidores Windows 2008, Windows 2012 e AD posteriores.

- `AD-SFU`

  Baseado nos Serviços do ative Directory para UNIX, esse esquema é apropriado para a maioria dos servidores do Windows 2003 e AD anteriores.

- `RFC-2307`

  Baseado em RFC-2307 (*an Approach for using LDAP as Network Information Service*), este esquema é apropriado para a maioria dos servidores UNIX AD.

c. Selecione vincular valores.

- `-min-bind-level {anonymous|simple|sasl}` especifica o nível mínimo de autenticação bind.

  O valor padrão é **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* especifica o usuário de vinculação.

  Para servidores do ative Directory, você deve especificar o usuário no formulário conta (DOMÍNIO/usuário) ou principal (user@domain.com). Caso contrário, você deve especificar o usuário em forma de nome distinto.

- `-bind-password` *`password`* especifica a senha de vinculação.

d. Selecione as opções de segurança da sessão, se necessário.

Pode ativar a assinatura e a selagem LDAP ou o LDAP através de TLS, se necessário pelo servidor LDAP.

- `--session-security {none|sign|seal}`

  Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

  Você também deve definir `-min-bind-level {sasl`, a menos que você queira que a autenticação de vinculação retorne **`anonymous`** ou **`simple`** se a vinculação de assinatura e vedação falhar.

- `-use-start-tls {true|`false`Selecione`

  Se definido como **`true`** e o servidor LDAP o suportar, o cliente LDAP utiliza uma ligação TLS encriptada ao servidor. O valor padrão é **`false`**. Você deve instalar um certificado de CA raiz autoassinado do servidor LDAP para usar essa opção.

Se a VM de armazenamento tiver um servidor SMB adicionado a um domínio e o servidor LDAP for um dos controladores de domínio do domínio inicial do servidor SMB, poderá modificar a `-session-security-for-ad-ldap` opção utilizando o `vserver cifs security modify` comando.

e. Selecione valores de porta, consulta e base.

Os valores padrão são recomendados, mas você deve verificar com o administrador LDAP se eles são apropriados para o seu ambiente.

- `-port` *`port`* Especifica a porta do servidor LDAP.

  O valor padrão é `389`.

Se pretender utilizar Iniciar TLS para proteger a ligação LDAP, tem de utilizar a porta predefinida 389. Iniciar TLS começa como uma conexão de texto simples através da porta padrão LDAP 389, e essa conexão é então atualizada para TLS. Se você alterar a porta, Iniciar TLS falhará.

- `-query-timeout` *`integer`* especifica o tempo limite da consulta em segundos.

  O intervalo permitido é de 1 a 10 segundos. O valor padrão é `3` segundos.

- `-base-dn` *`LDAP_DN`* Especifica o DN base.

  Vários valores podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada). O valor padrão é `""` (root).

- `-base-scope` {`base`|`onelevel`|`subtree`especifica o escopo de pesquisa base.

  O valor padrão é `subtree`.

- `-referral-enabled` {`true`|`false`Especifica se a busca por referência LDAP está ativada.

  A partir do ONTAP 9.5, isso permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP for retornada pelo servidor LDAP primário indicando que os Registros desejados estão presentes nos servidores LDAP referidos. O valor padrão é **`false`**.

Para pesquisar Registros presentes nos servidores LDAP referidos, o base-DN dos Registros referidos deve ser adicionado ao base-DN como parte da configuração do cliente LDAP.

2. Crie uma configuração de cliente LDAP na VM de armazenamento:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

Você deve fornecer o nome da VM de armazenamento ao criar uma configuração de cliente LDAP.

3. Verifique se a configuração do cliente LDAP foi criada com sucesso:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Exemplos

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP no qual a assinatura e a vedação são necessárias, e a descoberta de servidor LDAP é restrita a um site específico para o domínio especificado:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP onde a busca por referência LDAP é necessária:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1 especificando o DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1, ativando a busca de referência:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associe a configuração do cliente LDAP a SVMs

Para ativar o LDAP em um SVM, você deve usar o `vserver services name-service ldap create` comando para associar uma configuração de cliente LDAP ao SVM.

O que você vai precisar

- Um domínio LDAP já deve existir na rede e deve estar acessível ao cluster no qual o SVM está localizado.
- Uma configuração de cliente LDAP deve existir no SVM.

Passos

1. Ative o LDAP no SVM:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > ⓘ A partir do ONTAP 9.2, o `vserver services name-service ldap create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

   O comando a seguir habilita o LDAP no "VS1"SVM e o configura para usar a configuração de cliente LDAP "ldap1":

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Valide o status dos servidores de nomes usando o comando de verificação ldap do serviço de nomes dos serviços vserver.

   O comando a seguir valida servidores LDAP no SVM VS1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                   |
```

O comando name Service check está disponível a partir de ONTAP 9.2.

Verifique as fontes LDAP na tabela do switch do serviço de nomes

Você deve verificar se as fontes LDAP para serviços de nome estão listadas corretamente na tabela de opções de serviço de nomes para o SVM.

Passos

1. Exibir o conteúdo da tabela de opções de serviço de nomes atual:

   `vserver services name-service ns-switch show -vserver svm_name`

   O comando a seguir mostra os resultados do SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

   `namemap` especifica as fontes para procurar informações de mapeamento de nomes e em que ordem. Em um ambiente somente UNIX, essa entrada não é necessária. O mapeamento de nomes só é necessário em um ambiente misto usando UNIX e Windows.

2. Atualize a `ns-switch` entrada conforme apropriado:

Se quiser atualizar a entrada ns-switch para…	Digite o comando…
Informações do utilizador	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

Se quiser atualizar a entrada ns-switch para…	Digite o comando…
Informações do grupo	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Informações do netgroup	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Use Kerberos com NFS para segurança forte

Visão geral do uso do Kerberos com NFS para segurança forte

Se o Kerberos for usado em seu ambiente para autenticação forte, você precisará trabalhar com o administrador do Kerberos para determinar os requisitos e as configurações apropriadas do sistema de armazenamento e, em seguida, ativar o SVM como um cliente Kerberos.

Seu ambiente deve atender às seguintes diretrizes:

- A implantação do seu site deve seguir as práticas recomendadas para a configuração do servidor Kerberos e do cliente antes de configurar o Kerberos para ONTAP.
- Se possível, use NFSv4 ou posterior se a autenticação Kerberos for necessária.

  NFSv3 pode ser usado com Kerberos. No entanto, os benefícios completos de segurança do Kerberos só são realizados em implantações ONTAP de NFSv4 ou posterior.

- Para promover o acesso redundante ao servidor, o Kerberos deve ser habilitado em várias LIFs de dados em vários nós no cluster usando o mesmo SPN.
- Quando o Kerberos está habilitado no SVM, um dos seguintes métodos de segurança deve ser especificado em regras de exportação para volumes ou qtrees, dependendo da configuração do cliente NFS.
  - `krb5` (Protocolo Kerberos v5)
  - `krb5i` (Protocolo Kerberos v5 com verificação de integridade usando checksums)
  - `krb5p` (Protocolo Kerberos v5 com serviço de privacidade)

Além do servidor Kerberos e clientes, os seguintes serviços externos devem ser configurados para que o ONTAP suporte Kerberos:

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como o ative Directory ou o OpenLDAP, configurado para usar LDAP em SSL/TLS. Não use NIS, cujos pedidos são enviados em texto não criptografado e, portanto, não são seguros.

- NTP

  Você deve ter um servidor de tempo de trabalho executando NTP. Isso é necessário para evitar a falha de

autenticação Kerberos devido ao desvio de tempo.

- Resolução de nome de domínio (DNS)

  Cada cliente UNIX e cada SVM LIF devem ter um Registro de serviço (SRV) adequado registrado no KDC em zonas de pesquisa direta e inversa. Todos os participantes devem ser solucionáveis corretamente via DNS.

Verifique as permissões para a configuração Kerberos

O Kerberos requer que certas permissões UNIX sejam definidas para o volume raiz do SVM e para usuários e grupos locais.

Passos

1. Exiba as permissões relevantes no volume raiz da SVM:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   O volume raiz do SVM precisa ter a seguinte configuração:

Nome…	A definir…
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	755

   Se esses valores não forem exibidos, use o `volume modify` comando para atualizá-los.

2. Exibir os usuários locais do UNIX:

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS. O primeiro componente do usuário cliente NFS SPN é usado como usuário. O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.
raiz	0	0	Necessário para a montagem.

Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-user modify` comando para atualizá-los.

3. Exibir os grupos UNIX locais:

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0

Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-group modify` comando para atualizá-los.

Crie uma configuração NFS Kerberos realm

Se você quiser que o ONTAP acesse servidores Kerberos externos em seu ambiente, primeiro configure o SVM para usar um realm Kerberos existente. Para fazer isso, você precisa reunir valores de configuração para o servidor KDC Kerberos e, em seguida, usar o `vserver nfs kerberos realm create` comando para criar a configuração de realm Kerberos em um SVM.

O que você vai precisar

O administrador do cluster deve ter configurado o NTP no sistema de armazenamento, cliente e servidor KDC para evitar problemas de autenticação. As diferenças de tempo entre um cliente e um servidor (desvio de relógio) são uma causa comum de falhas de autenticação.

Passos

1. Consulte o administrador do Kerberos para determinar os valores de configuração apropriados para fornecer com o `vserver nfs kerberos realm create` comando.
2. Crie uma configuração de realm Kerberos no SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Verifique se a configuração do realm Kerberos foi criada com sucesso:

   `vserver nfs kerberos realm show`

Exemplos

O comando a seguir cria uma configuração NFS Kerberos Realm para o SVM VS1 que usa um servidor Microsoft ative Directory como servidor KDC. O Reino Kerberos é AUTH.EXAMPLE.COM. O servidor do ative Directory tem o nome ad-1 e seu endereço IP é 10.10.8.14. O desvio de relógio permitido é de 300 segundos (o padrão). O endereço IP do servidor KDC é 10.10.8.14, e seu número de porta é 88 (o padrão). "Configuração do Microsoft Kerberos" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

O comando a seguir cria uma configuração NFS Kerberos realm para o SVM VS1 que usa um MIT KDC. O Reino Kerberos é SECURITY.EXAMPLE.COM. A inclinação permitida do relógio é de 300 segundos. O endereço IP do servidor KDC é 10.10.9.1, e seu número de porta é 88. O fornecedor KDC é outro para indicar um fornecedor UNIX. O endereço IP do servidor administrativo é 10.10.9.1, e seu número de porta é 749 (o padrão). O endereço IP do servidor de senhas é 10.10.9.1, e seu número de porta é 464 (o padrão). "UNIX Kerberos config" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar os tipos de criptografia permitidos do NFS Kerberos

Por padrão, o ONTAP oferece suporte aos seguintes tipos de criptografia para o Kerberos NFS: DES, 3DES, AES-128 e AES-256. Você pode configurar os tipos de criptografia permitidos para cada SVM de acordo com os requisitos de segurança do seu ambiente específico usando o `vserver nfs modify` comando com o `-permitted -enc-types` parâmetro.

Sobre esta tarefa

Para maior compatibilidade com clientes, o ONTAP suporta criptografia DES fraca e AES forte por padrão. Isso significa, por exemplo, que se você quiser aumentar a segurança e seu ambiente a suportar, você pode usar este procedimento para desativar DES e 3DES e exigir que os clientes usem apenas criptografia AES.

Você deve usar a criptografia mais forte disponível. Para ONTAP, isso é AES-256. Deve confirmar com o administrador do KDC que este nível de encriptação é suportado no seu ambiente.

- Ativar ou desativar totalmente AES (AES-128 e AES-256) em SVMs é disruptivo porque destrói o arquivo DES principal/keytab original, exigindo assim que a configuração Kerberos seja desativada em todos os LIFs para o SVM.

  Antes de fazer essa alteração, você deve verificar se os clientes NFS não dependem da criptografia AES no SVM.

- Ativar ou desativar DES ou 3DES não requer alterações na configuração Kerberos em LIFs.

Passo

1. Ative ou desative o tipo de encriptação permitido que pretende:

Se quiser ativar ou desativar…	Siga estes passos…
DES ou 3DES	a. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separe vários tipos de criptografia com uma vírgula. b. Verifique se a alteração foi bem-sucedida `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Se quiser ativar ou desativar…	Siga estes passos…

AES-128 ou AES-256	a. Identifique em que SVM e LIF Kerberos estão ativados
	`vserver nfs kerberos interface show`
	b. Desative o Kerberos em todos os LIFs no SVM cujo tipo de criptografia NFS Kerberos permitido você deseja modificar
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	c. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	Separe vários tipos de criptografia com uma vírgula.
	d. Verifique se a alteração foi bem-sucedida
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	e. Reative o Kerberos em todos os LIFs na SVM
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	f. Verifique se o Kerberos está ativado em todos os LIFs
	`vserver nfs kerberos interface show`

Ative o Kerberos em um LIF de dados

Você pode usar o `vserver nfs kerberos interface enable` comando para habilitar o Kerberos em um LIF de dados. Isso permite que o SVM use os serviços de segurança Kerberos para NFS.

Sobre esta tarefa

Se você estiver usando um KDC do ative Directory, os primeiros 15 carateres de qualquer SPNs usados devem ser exclusivos em SVMs dentro de um Reino ou domínio.

Passos

1. Crie a configuração NFS Kerberos:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   O ONTAP requer a chave secreta para o SPN do KDC para habilitar a interface Kerberos.

Para os KDCs da Microsoft, o KDC é contatado e um prompt de nome de usuário e senha são emitidos na CLI para obter a chave secreta. Se você precisar criar o SPN em uma ou diferente do realm Kerberos, você poderá especificar o parâmetro opcional `-ou`.

Para KDCs não Microsoft, a chave secreta pode ser obtida usando um de dois métodos:

Se você…	Você também deve incluir o seguinte parâmetro com o comando…
Peça às credenciais do administrador do KDC para recuperar a chave diretamente do KDC	`-admin-username` *kdc_admin_username*
Não tem as credenciais de administrador do KDC, mas tem um arquivo keytab do KDC que contém a chave	`-keytab-uri` digite seu comentário aqui:// *uri*

2. Verifique se o Kerberos foi ativado no LIF:

   `vserver nfs kerberos-config show`

3. Repita as etapas 1 e 2 para ativar o Kerberos em várias LIFs.

Exemplo

O comando a seguir cria e verifica uma configuração NFS Kerberos para o SVM chamado VS1 na interface lógica ves03-D1, com o SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM na ou lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Use o TLS com NFS para ter uma segurança forte

Visão geral do uso do TLS com NFS para uma segurança forte

O TLS permite comunicações de rede criptografadas com segurança equivalente e menos complexidade do que o Kerberos e o IPsec. Como administrador, você pode habilitar, configurar e desabilitar o TLS para segurança forte com conexões NFSv3 e NFSv4.x usando o Gerenciador de sistema, a CLI do ONTAP ou a API REST do ONTAP.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

O ONTAP usa o TLS 1,3 para conexões NFS em TLS.

Requisitos

O NFS em TLS requer certificados X,509. Você pode criar e instalar um certificado de servidor assinado pela CA no cluster do ONTAP ou instalar um certificado que o serviço NFS usa diretamente. Seus certificados devem atender às seguintes diretrizes:

- O nome comum (CN) de cada certificado deve ser configurado com o nome de domínio totalmente qualificado (FQDN) do LIF de dados no qual o TLS será ativado.
- O nome alternativo do assunto (SAN) de cada certificado deve ser configurado com o endereço IP do LIF de dados no qual o TLS será ativado. Opcionalmente, você pode configurar a SAN com o endereço IP e o FQDN do LIF de dados. Se o endereço IP e o FQDN estiverem configurados, os clientes NFS podem se conetar usando o endereço IP ou o FQDN.
- Você pode instalar vários certificados de serviço NFS para o mesmo LIF, mas apenas um deles pode ser usado de cada vez como parte da configuração TLS NFS.

Ativar ou desativar TLS para clientes NFS no ONTAP

Você pode ativar ou desativar o TLS em um data LIF para clientes NFS. Quando você ativa o NFS em TLS, o SVM usa o TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

- Consulte "requisitos"o para NFS sobre TLS antes de começar.
- Saiba mais sobre o "ativação da interface nfs tls do svm" comando na referência de comando ONTAP.

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) na qual ativar o TLS.
2. Habilite o TLS para conexões NFS nessa VM e interface de storage. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir habilita o NFS sobre TLS no `data1` LIF da `vs1` VM de storage:

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

> Quando você desativa o NFS em TLS, o certificado TLS usado para a conexão NFS é removido. Se você precisar habilitar o NFS em TLS no futuro, precisará especificar novamente um nome de certificado durante a capacitação.

Antes de começar

Saiba mais sobre o "desativação da interface nfs tls do svm" comando na referência de comando ONTAP.

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) para desativar o TLS.
2. Desative TLS para conexões NFS nessa VM e interface de storage. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir desativa NFS sobre TLS no `data1` LIF da `vs1` VM de armazenamento:

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Editar uma configuração TLS

Você pode alterar as configurações de uma configuração NFS em TLS existente. Por exemplo, você pode usar este procedimento para atualizar o certificado TLS.

Antes de começar

Saiba mais sobre o "modificação da interface tls nfs do svm" comando na referência de comando ONTAP.

Passos

1. Escolha uma VM de storage e uma interface lógica (LIF) para modificar a configuração TLS para clientes NFS.
2. Modificar a configuração. Se especificar um `status` de `enable`, também terá de especificar o `certificate-name` parâmetro. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir modifica a configuração NFS sobre TLS no `data2` LIF da `vs2` VM de armazenamento:

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```

Adicionar capacidade de storage a um SVM habilitado para NFS

Adicionar capacidade de storage a uma visão geral da SVM habilitada para NFS

Para adicionar capacidade de storage a um SVM habilitado para NFS, você precisa criar um volume ou qtree para fornecer um contêiner de storage e criar ou modificar uma política de exportação para esse contêiner. Em seguida, você pode verificar o acesso do cliente NFS a partir do cluster e testar o acesso a partir de sistemas cliente.

O que você vai precisar

- O NFS precisa estar completamente configurado no SVM.
- A política de exportação padrão do volume raiz da SVM deve conter uma regra que permita acesso a todos os clientes.
- Todas as atualizações da configuração dos serviços de nome devem estar concluídas.
- Quaisquer adições ou modificações a uma configuração Kerberos devem estar concluídas.

Crie uma política de exportação

Antes de criar regras de exportação, você deve criar uma política de exportação para mantê-las. Você pode usar o `vserver export-policy create` comando para criar uma política de exportação.

Passos

1. Criar uma política de exportação:

   ```
   vserver export-policy create -vserver vserver_name -policyname policy_name
   ```

O nome da política pode ter até 256 carateres.

2. Verifique se a política de exportação foi criada:

   `vserver export-policy show -policyname policy_name`

Exemplo

Os comandos a seguir criam e verificam a criação de uma política de exportação chamada exp1 no SVM chamado VS1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Adicione uma regra a uma política de exportação

Sem regras, a política de exportação não pode fornecer acesso de cliente aos dados. Para criar uma nova regra de exportação, você deve identificar clientes e selecionar um formato de correspondência de cliente, selecionar os tipos de acesso e segurança, especificar um mapeamento de ID de usuário anônimo, selecionar um número de índice de regras e selecionar o protocolo de acesso. Em seguida, você pode usar o `vserver export-policy rule create` comando para adicionar a nova regra a uma política de exportação.

O que você vai precisar

- A política de exportação à qual deseja adicionar as regras de exportação já deve existir.
- O DNS deve ser configurado corretamente nos dados SVM e os servidores DNS devem ter entradas corretas para clientes NFS.

  Isso ocorre porque o ONTAP executa pesquisas de DNS usando a configuração DNS do SVM de dados para determinados formatos de correspondência de clientes, e falhas na correspondência de regras de política de exportação podem impedir o acesso aos dados do cliente.

- Se você estiver autenticando com Kerberos, você deve ter determinado qual dos seguintes métodos de segurança é usado em seus clientes NFS:
  - `krb5` (Protocolo Kerberos V5)
  - `krb5i` (Protocolo Kerberos V5 com verificação de integridade usando checksums)
  - `krb5p` (Protocolo Kerberos V5 com serviço de privacidade)

Sobre esta tarefa

Não é necessário criar uma nova regra se uma regra existente em uma política de exportação abranger seus requisitos de correspondência de cliente e acesso.

Se você estiver autenticando com Kerberos e se todos os volumes da SVM forem acessados por Kerberos,

poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5`, `krb5i` ou `krb5p`.

Passos

1. Identificar os clientes e o formato de correspondência do cliente para a nova regra.

   A `-clientmatch` opção especifica os clientes aos quais a regra se aplica. Valores de correspondência de cliente único ou múltiplo podem ser especificados; as especificações de vários valores devem ser separadas por vírgulas. Você pode especificar a correspondência em qualquer um dos seguintes formatos:

Formato de correspondência do cliente	Exemplo
Nome de domínio precedido pelo caractere "."	`.example.com` ou `.example.com,.example.net,...`
Nome do host	`host1` ou `host1,host2, ...`
Endereço IPv4	`10.1.12.24` ou `10.1.12.24,10.1.12.25, ...`
Endereço IPv4 com uma máscara de sub-rede expressa como um número de bits	`10.1.12.10/4` ou `10.1.12.10/4,10.1.12.11/4,...`
Endereço IPv4 com uma máscara de rede	`10.1.16.0/255.255.255.0` ou `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Endereço IPv6 no formato pontilhado	`::1.2.3.4` ou `::1.2.3.4,::1.2.3.5,...`
Endereço IPv6 com uma máscara de sub-rede expressa como um número de bits	`ff::00/32` ou `ff::00/32,ff::01/32,...`
Um único netgroup com o nome netgroup precedido pelo caractere at	`@netgroup1` ou `@netgroup1,@netgroup2,...`

   Você também pode combinar tipos de definições de cliente; por exemplo `.example.com,@netgroup1,.`

   Ao especificar endereços IP, observe o seguinte:

   - Não é permitido introduzir um intervalo de endereços IP, como 10,1.12,10-10,1.12,70.

     As entradas neste formato são interpretadas como uma cadeia de texto e tratadas como um nome de host.

   - Ao especificar endereços IP individuais em regras de exportação para gerenciamento granular do acesso do cliente, não especifique endereços IP que sejam atribuídos dinamicamente (por exemplo, DHCP) ou temporariamente (por exemplo, IPv6).

     Caso contrário, o cliente perde o acesso quando seu endereço IP muda.

- Não é permitido inserir um endereço IPv6 com uma máscara de rede, como ff::12/FF::00.

2. Selecione os tipos de acesso e segurança para correspondências de clientes.

   Você pode especificar um ou mais dos seguintes modos de acesso aos clientes que se autenticam com os tipos de segurança especificados:

   - `-rorule` (acesso somente leitura)
   - `-rwrule` (acesso de leitura e gravação)
   - `-superuser` (acesso à raiz)

   > Um cliente só pode obter acesso de leitura e gravação para um tipo de segurança específico se a regra de exportação também permitir acesso somente leitura para esse tipo de segurança. Se o parâmetro somente leitura for mais restritivo para um tipo de segurança do que o parâmetro leitura-gravação, o cliente poderá não obter acesso de leitura-gravação. O mesmo se aplica ao acesso do superusuário.

   Você pode especificar uma lista separada por vírgulas de vários tipos de segurança para uma regra. Se especificar o tipo de segurança `any` como ou `never`, não especifique outros tipos de segurança. Escolha entre os seguintes tipos de segurança válidos:

Quando o tipo de segurança está definido como…	Um cliente correspondente pode acessar os dados exportados…
`any`	Sempre, independentemente do tipo de segurança de entrada.
`none`	Se listado sozinho, os clientes com qualquer tipo de segurança recebem acesso como anônimo. Se listado com outros tipos de segurança, os clientes com um tipo de segurança especificado recebem acesso e os clientes com qualquer outro tipo de segurança recebem acesso como anônimos.
`never`	Nunca, independentemente do tipo de segurança de entrada.
`krb5`	Se for autenticado pelo Kerberos 5. Somente autenticação: O cabeçalho de cada solicitação e resposta é assinado.
`krb5i`	Se for autenticado pelo Kerberos 5i. Autenticação e integridade: O cabeçalho e o corpo de cada solicitação e resposta são assinados.

Quando o tipo de segurança está definido como…	Um cliente correspondente pode acessar os dados exportados…
`krb5p`	Se for autenticado pelo Kerberos 5P. Autenticação, integridade e privacidade: O cabeçalho e o corpo de cada solicitação e resposta são assinados e a carga útil de dados NFS é criptografada.
`ntlm`	Se for autenticado pelo CIFS NTLM.
`sys`	Se for autenticado por NFS AUTH_SYS.

O tipo de segurança recomendado é `sys`, ou se o Kerberos for usado, `krb5` `krb5i` , ou `krb5p`.

Se você estiver usando Kerberos com NFSv3, a regra de política de exportação deverá permitir `-rorule` e `-rwrule` acessar `sys` além `krb5` do . Isso ocorre devido à necessidade de permitir o acesso do Network Lock Manager (NLM) à exportação.

3. Especifique um mapeamento de ID de usuário anônimo.

   A `-anon` opção especifica um ID de usuário UNIX ou nome de usuário que é mapeado para solicitações de cliente que chegam com um ID de usuário de 0 (zero), que normalmente é associado à raiz do nome de usuário. O valor padrão é `65534`. Os clientes NFS normalmente associam o ID de usuário 65534 ao nome de usuário nobody (também conhecido como *root squashing*). No ONTAP, esse ID de usuário está associado ao usuário pcuser. Para desativar o acesso por qualquer cliente com uma ID de usuário de 0, especifique um valor `65535` de .

4. Selecione a ordem do índice de regras.

   A `-ruleindex` opção especifica o número do índice para a regra. As regras são avaliadas de acordo com sua ordem na lista de números de índice; regras com números de índice mais baixos são avaliadas primeiro. Por exemplo, a regra com índice número 1 é avaliada antes da regra com índice número 2.

Se você está adicionando…	Então…
A primeira regra para uma política de exportação	Introduza `1`.
Regras adicionais para uma política de exportação	a. Exibir regras existentes na política `vserver export-policy rule show -instance -policyname` *`your_policy`* b. Selecione um número de índice para a nova regra, dependendo da ordem em que ela deve ser avaliada.

5. Selecione o valor de acesso NFS aplicável:{`nfs`|`nfs3`|`nfs4`.

   `nfs` corresponde a qualquer versão e `nfs3` `nfs4` corresponde apenas a essas versões específicas.

6. Crie a regra de exportação e adicione-a a uma política de exportação existente:

```
vserver export-policy rule create -vserver vserver_name -policyname
policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
"text,text,…" } -rorule security_type -rwrule security_type -superuser
security_type -anon user_ID
```

7. Exiba as regras da política de exportação para verificar se a nova regra está presente:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   O comando exibe um resumo para essa política de exportação, incluindo uma lista de regras aplicadas a essa política. O ONTAP atribui a cada regra um número de índice de regra. Depois de saber o número do índice da regra, você pode usá-lo para exibir informações detalhadas sobre a regra de exportação especificada.

8. Verifique se as regras aplicadas à política de exportação estão configuradas corretamente:

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Exemplos

Os comandos a seguir criam e verificam a criação de uma regra de exportação no SVM chamado VS1 em uma política de exportação chamada RS1. A regra tem o índice número 1. A regra corresponde a qualquer cliente no domínio eng.company.com e o netgroup netgroup1. A regra habilita todo o acesso NFS. Ele permite acesso somente leitura e leitura-gravação a usuários autenticados com AUTH_SYS. Os clientes com o ID de usuário UNIX 0 (zero) são anonimizados, a menos que autenticados com o Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                 Superuser Security Types: krb5
             Honor SetUID Bits in SETATTR: true
                Allow Creation of Devices: true
```

Os comandos a seguir criam e verificam a criação de uma regra de exportação no SVM chamado VS2 em uma política de exportação chamada expol2. A regra tem o índice número 21. A regra corresponde clientes aos membros do netgroup dev_netgroup_main. A regra habilita todo o acesso NFS. Ele permite acesso somente leitura para usuários autenticados com AUTH_SYS e requer autenticação Kerberos para leitura-gravação e acesso root. Os clientes com a ID de usuário UNIX 0 (zero) têm acesso root negado, a menos que autenticados com Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Crie um volume ou um contêiner de storage de qtree

Crie um volume

Você pode criar um volume e especificar seu ponto de junção e outras propriedades usando o `volume create` comando.

Sobre esta tarefa

Um volume deve incluir um *caminho de junção* para que seus dados sejam disponibilizados aos clientes. Você pode especificar o caminho de junção ao criar um novo volume. Se você criar um volume sem especificar um caminho de junção, será necessário *montar* o volume no namespace SVM usando o `volume mount` comando.

Antes de começar

- O NFS deve estar configurado e em execução.
- O estilo de segurança da SVM deve ser UNIX.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume com um ponto de junção:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   As opções para `-junction-path` são as seguintes:

   - Diretamente sob a raiz, por exemplo, */new_vol*

     Você pode criar um novo volume e especificar que ele seja montado diretamente no volume raiz da SVM.

   - Em um diretório existente, por exemplo, */existing_dir/new_vol*

     Você pode criar um novo volume e especificar que ele seja montado em um volume existente (em uma hierarquia existente), expresso como um diretório.

     Se você quiser criar um volume em um novo diretório (em uma nova hierarquia em um novo volume), por exemplo, */new_dir/new_vol* será necessário criar primeiro um novo volume pai que seja juntado ao volume raiz SVM. Em seguida, você criaria o novo volume filho no caminho de junção do novo volume pai (novo diretório).

   Se você pretende usar uma política de exportação existente, você pode especificá-la quando você cria o volume. Você também pode adicionar uma política de exportação mais tarde com o `volume modify` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado:

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Exemplos

O comando a seguir cria um novo volume chamado users1 no SVM vs1.example.com e no agregado aggr1. O novo volume é disponibilizado em `/users`. O volume tem 750 GB de tamanho e sua garantia de volume é do tipo volume (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

O comando a seguir cria um novo volume chamado "home4" no SVM "vs1.example.com" e o agregado "aggr1". O diretório `/eng/` já existe no namespace para o VS1 SVM, e o novo volume é disponibilizado no `/eng/home`, que se torna o diretório home do `/eng/` namespace. O volume é de 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- -------  -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Crie uma qtree

Você pode criar uma qtree para conter seus dados e especificar suas propriedades usando o `volume qtree create` comando.

O que você vai precisar

- O SVM e o volume que conterá a nova qtree já devem existir.
- O estilo de segurança da SVM deve ser UNIX, e o NFS deve ser configurado e executado.

Passos

1. Crie a qtree:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Você pode especificar o volume e a qtree como argumentos separados ou especificar o argumento de caminho de qtree no formato `/vol/`*`volume_name/_qtree_name`*.

   Por padrão, qtrees herdam as políticas de exportação de seu volume pai, mas eles podem ser configurados para usar suas próprias políticas. Se você pretende usar uma política de exportação existente, pode especificá-la quando criar a qtree. Você também pode adicionar uma política de exportação mais tarde com o `volume qtree modify` comando.

2. Verifique se a qtree foi criada com o caminho de junção desejado:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Exemplo

O exemplo a seguir cria uma qtree chamada qt01 localizada no SVM vs1.example.com que tem um caminho de junção `/vol/data1` :

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Proteja o acesso NFS usando políticas de exportação

Proteja o acesso NFS usando políticas de exportação

Você pode usar políticas de exportação para restringir o acesso NFS a volumes ou qtrees a clientes que correspondem a parâmetros específicos. Ao provisionar um novo storage, você pode usar uma política e regras existentes, adicionar regras a uma política existente ou criar uma nova política e regras. Você também pode verificar a configuração das políticas de exportação

> A partir do ONTAP 9.3, você pode habilitar a verificação de configuração de política de exportação como uma tarefa em segundo plano que Registra quaisquer violações de regras em uma lista de regras de erro. Os `vserver export-policy config-checker` comandos invocam o verificador e exibem resultados, que podem ser usados para verificar sua configuração e excluir regras errôneas da política.os comandos validam somente a configuração de exportação para nomes de host, netgroups e usuários anônimos.

Gerenciar a ordem de processamento das regras de exportação

Você pode usar o `vserver export-policy rule setindex` comando para definir manualmente o número de índice de uma regra de exportação existente. Isso permite que você especifique a precedência pela qual o ONTAP aplica regras de exportação para solicitações de cliente.

Sobre esta tarefa

Se o novo número de índice já estiver em uso, o comando insere a regra no local especificado e reordena a lista de acordo.

Passo

1. Modifique o número de índice de uma regra de exportação especificada:

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Exemplo

O comando a seguir altera o número de índice de uma regra de exportação no número de índice 3 para o número de índice 2 em uma política de exportação chamada RS1 no SVM chamado VS1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Atribua uma política de exportação a um volume

Cada volume contido no SVM deve estar associado a uma política de exportação que contenha regras de exportação para que os clientes acessem os dados no volume.

Sobre esta tarefa

Você pode associar uma política de exportação a um volume ao criar o volume ou a qualquer momento depois de criar o volume. Você pode associar uma política de exportação ao volume, embora uma política possa ser associada a muitos volumes.

Passos

1. Se uma política de exportação não foi especificada quando o volume foi criado, atribua uma política de exportação ao volume:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Verifique se a política foi atribuída ao volume:

   ```
   volume show -volume volume_name -fields policy
   ```

Exemplo

Os comandos a seguir atribuem a política de exportação nfs_policy ao volume vol1 no SVM VS1 e verificam a atribuição:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Atribua uma política de exportação a uma qtree

Em vez de exportar um volume inteiro, você também pode exportar uma qtree específica em um volume para torná-lo diretamente acessível aos clientes. Você pode exportar uma qtree atribuindo uma política de exportação a ela. Você pode atribuir a política de exportação ao criar uma nova qtree ou modificando uma qtree existente.

O que você vai precisar

A política de exportação tem de existir.

Sobre esta tarefa

Por padrão, qtrees herdam a política de exportação pai do volume contendo se não for especificado de outra forma no momento da criação.

Você pode associar uma política de exportação a uma qtree quando você cria a qtree ou a qualquer momento depois de criar a qtree. Você pode associar uma política de exportação à qtree, embora uma política possa ser associada a muitos qtrees.

Passos

1. Se uma política de exportação não foi especificada quando a qtree foi criada, atribua uma política de exportação à qtree:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. Verifique se a política foi atribuída à qtree:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Exemplo

Os comandos a seguir atribuem a política de exportação nfs_policy à qtree qt1 no SVM VS1 e verificam a atribuição:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Verifique o acesso do cliente NFS a partir do cluster

Você pode dar a clientes selecionados acesso ao compartilhamento definindo permissões de arquivo UNIX em um host de administração UNIX. Você pode verificar o acesso do cliente usando o `vserver export-policy check-access` comando, ajustando as regras de exportação conforme necessário.

Passos

1. No cluster, verifique o acesso do cliente às exportações usando o `vserver export-policy check-access` comando.

   O comando a seguir verifica o acesso de leitura/gravação para um cliente NFSv3 com o endereço IP 1.2.3.4 para o volume Home2. O comando output mostra que o volume usa a política de exportação `exp-home-dir` e que o acesso é negado.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                    Policy    Policy     Rule
Path                    Policy      Owner     Owner Type Index  Access
----------------------- ----------- --------- ---------- ------
----------
/                       default     vs1_root  volume          1 read
/eng                    default     vs1_root  volume          1 read
/eng/home2              exp-home-dir home2    volume          1 denied

3 entries were displayed.
```

2. Examine a saída para determinar se a política de exportação funciona conforme o pretendido e o acesso do cliente se comporta como esperado.

   Especificamente, você deve verificar qual política de exportação é usada pelo volume ou qtree e o tipo de acesso que o cliente tem como resultado.

3. Se necessário, reconfigure as regras da política de exportação.

Testar o acesso NFS a partir de sistemas cliente

Depois de verificar o acesso NFS ao novo objeto de storage, você deve testar a configuração fazendo login em um host de administração NFS, lendo e gravando dados no SVM. Você deve repetir o processo como um usuário não-root em um sistema cliente.

O que você vai precisar

- O sistema cliente deve ter um endereço IP permitido pela regra de exportação especificada anteriormente.
- Você deve ter as informações de login para o usuário root.

Passos

1. No cluster, verifique o endereço IP do LIF que está hospedando o novo volume:

   `network interface show –vserver` *`svm_name`*

2. Faça login como o usuário raiz no sistema de cliente de host de administração.
3. Altere o diretório para a pasta de montagem:

   `cd /mnt/`

4. Crie e monte uma nova pasta usando o endereço IP do SVM:

   a. Criar uma nova pasta
   `mkdir /mnt/folder`

   b. Monte o novo volume neste novo diretório
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Mude o diretório para a nova pasta
   `cd folder`

   Os comandos a seguir criam uma pasta chamada test1, montam o volume vol1 no endereço IP 192.0.2.130 na pasta de montagem test1 e mudam para o novo diretório test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Crie um novo arquivo, verifique se ele existe e escreva texto nele:

   a. Criar um arquivo de teste
   `touch filename`

   b. Verifique se o arquivo existe
   `ls -l filename`

   c. Digite
   `cat > filename`

   Digite algum texto e pressione Ctrl-D para escrever texto no arquivo de teste.

   d. Exibir o conteúdo do arquivo de teste. E
   `cat filename`

   e. Remova o arquivo de teste
   `rm filename`

   f. Retornar para o diretório pai
   `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Como root, defina qualquer propriedade e permissões UNIX desejadas no volume montado.

7. Em um sistema cliente UNIX identificado em suas regras de exportação, faça login como um dos usuários autorizados que agora tem acesso ao novo volume e repita os procedimentos nas etapas 3 a 5 para verificar se você pode montar o volume e criar um arquivo.

Onde encontrar informações adicionais

Depois de testar com êxito o acesso ao cliente NFS, você pode executar uma configuração NFS adicional ou adicionar acesso SAN. Quando o acesso ao protocolo estiver concluído, você deverá proteger o volume raiz da máquina virtual de storage (SVM).

Configuração NFS

Você pode configurar ainda mais o acesso NFS usando as seguintes informações e relatórios técnicos:

- "Gerenciamento de NFS"

  Descreve como configurar e gerenciar o acesso a arquivos usando NFS.

- "Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"

  Serve como um guia operacional NFSv3 e NFSv4 e fornece uma visão geral do sistema operacional ONTAP com foco em NFSv4.

- "Relatório técnico da NetApp 4073: Autenticação unificada segura"

  Explica como configurar o ONTAP para uso com servidores Kerberos baseados em UNIX versão 5 (krb5) para autenticação de armazenamento NFS e AD (AD) como provedor de identidade KDC e LDAP (Lightweight Directory Access Protocol).

- "Relatório técnico da NetApp 3580: NFSv4 melhorias e melhores práticas Guia de implementação do Data ONTAP"

  Descreve as práticas recomendadas que devem ser seguidas durante a implementação de componentes NFSv4 em clientes AIX, Linux ou Solaris conetados a sistemas que executam o ONTAP.

Configuração de rede

Você pode configurar ainda mais recursos de rede e serviços de nome usando as seguintes informações e relatórios técnicos:

- "Gerenciamento de NFS"

  Descreve como configurar e gerenciar redes ONTAP.

- "Relatório técnico da NetApp 4182: Considerações sobre o projeto de armazenamento Ethernet e práticas recomendadas para configurações de Data ONTAP em cluster"

  Descreve a implementação das configurações de rede ONTAP e fornece cenários comuns de implantação de rede e recomendações de práticas recomendadas.

- "Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

  Explica como configurar LDAP, NIS, DNS e configuração de arquivos locais para fins de autenticação.

Configuração do protocolo SAN

Se quiser fornecer ou modificar o acesso SAN ao novo SVM, você pode usar as informações de configuração FC ou iSCSI, que estão disponíveis para vários sistemas operacionais de host.

Proteção do volume raiz

Depois de configurar protocolos no SVM, você deve garantir que seu volume raiz esteja protegido:

- "Proteção de dados"

  Descreve como criar um espelhamento de compartilhamento de carga para proteger o volume raiz da SVM, que é uma prática recomendada do NetApp para SVMs habilitadas para nas. Também descreve como recuperar rapidamente de falhas ou perdas de volume promovendo o volume raiz do SVM a partir de um espelhamento de compartilhamento de carga.

Como as exportações do ONTAP diferem das exportações do modo 7

Como as exportações do ONTAP diferem das exportações do modo 7

Se não estiver familiarizado com a forma como o ONTAP implementa as exportações de NFS, pode comparar as ferramentas de configuração de exportação de modo 7D e ONTAP, bem como exemplos de arquivos de modo 7D `/etc/exports` com políticas e regras em cluster.

No ONTAP não há `/etc/exports` nenhum arquivo e nenhum `exportfs` comando. Em vez disso, você deve definir uma política de exportação. As políticas de exportação permitem que você controle o acesso do cliente da mesma forma que você fez no modo 7, mas oferecem funcionalidades adicionais, como a capacidade de reutilizar a mesma política de exportação para vários volumes.

Informações relacionadas

"Gerenciamento de NFS"

"Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"

Comparação de exportações em modo 7D e ONTAP

As exportações no ONTAP são definidas e usadas de forma diferente do que em ambientes de 7 modos.

Áreas de diferença	Modo 7D.	ONTAP
Como as exportações são definidas	As exportações são definidas `/etc/exports` no arquivo.	As exportações são definidas criando uma política de exportação em um SVM. O SVM pode incluir mais de uma política de exportação.

Âmbito de exportação	• As exportações se aplicam a um caminho ou qtree de arquivo especificado. • Você deve criar uma entrada separada em `/etc/exports` para cada caminho ou qtree de arquivo. • As exportações são persistentes somente se forem definidas no `/etc/exports` arquivo.	• As políticas de exportação se aplicam a um volume inteiro, incluindo todos os caminhos de arquivo e qtrees contidos no volume. • As políticas de exportação podem ser aplicadas a mais de um volume, se desejar. • Todas as políticas de exportação são persistentes nas reinicializações do sistema.
Esgrima (especificando acesso diferente para clientes específicos aos mesmos recursos)	Para fornecer a clientes específicos acesso diferente a um único recurso exportado, você tem que listar cada cliente e seu acesso permitido no `/etc/exports` arquivo.	As políticas de exportação são compostas por várias regras de exportação individuais. Cada regra de exportação define permissões de acesso específicas para um recurso e lista os clientes que têm essas permissões. Para especificar um acesso diferente para clientes específicos, você precisa criar uma regra de exportação para cada conjunto específico de permissões de acesso, listar os clientes que têm essas permissões e, em seguida, adicionar as regras à política de exportação.
Alias de nome	Ao definir uma exportação, pode optar por tornar o nome da exportação diferente do nome do caminho do ficheiro. Você deve usar o `-actual` parâmetro ao definir tal exportação no `/etc/exports` arquivo.	Pode optar por tornar o nome do volume exportado diferente do nome do volume real. Para fazer isso, é necessário montar o volume com um nome de caminho de junção personalizado no namespace SVM. Por padrão, os volumes são montados com seu nome de volume. Para personalizar o nome do caminho de junção de um volume, você precisa desmontá-lo, renomeá-lo e remontá-lo.

Exemplos de políticas de exportação do ONTAP

Você pode revisar exemplos de políticas de exportação para entender melhor como as políticas de exportação funcionam no ONTAP.

Exemplo de implementação do ONTAP de uma exportação de 7 modos

O exemplo a seguir mostra uma exportação do modo 7 como aparece no `/etc/export` arquivo:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Para reproduzir essa exportação como uma política de exportação em cluster, você precisa criar uma política de exportação com três regras de exportação e atribuir a política de exportação ao volume vol1.

Regra	Elemento	Valor
Regra 1	`-clientmatch` (especificação do cliente)	`@readonly_netgroup`
`-ruleindex`(posição da regra de exportação na lista de regras)	`1`	`-protocol`
`nfs`	`-rorule`(permitir acesso somente leitura)	`sys` (Cliente autenticado com AUTH_SYS)
`-rwrule`(permitir acesso de leitura e gravação)	`never`	`-superuser`(permitir acesso ao superusuário)
`none`(root *squashed* para anon)	Regra 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Regra 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`

Regra	Elemento	Valor
sys	-superuser	none

1. Crie uma política de exportação chamada exp_vol1:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Crie três regras com os seguintes parâmetros para o comando base:
   - Base de comando
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - Parâmetros da regra
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`

3. Atribua a política ao volume vol1:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Consolidação de amostra de exportações de 7 modos

O exemplo a seguir mostra um arquivo de 7 modos `/etc/export` que inclui uma linha para cada um dos 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

No ONTAP, uma de duas políticas é necessária para cada qtree: Uma com uma regra que inclui `-clientmatch host1519s`, ou outra com uma regra que `-clientmatch host2057s`inclui .

1. Crie duas políticas de exportação chamadas exp_vol1q1 e exp_vol1q2:
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Crie uma regra para cada política:
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1`

```
-clientmatch host1519s -rwrule sys -superuser sys
```

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Aplique as políticas ao qtrees:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [next 4 qtrees…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [next 4 qtrees…]

Se você precisar adicionar qtrees adicionais para esses hosts mais tarde, você usaria as mesmas políticas de exportação.

Gerencie o NFS com a CLI

Visão geral de referência de NFS

O ONTAP inclui recursos de acesso a arquivos disponíveis para o protocolo NFS. Você pode habilitar um servidor NFS e exportar volumes ou qtrees.

Você executa este procedimento nas seguintes circunstâncias:

- Você quer entender a variedade de funcionalidades do protocolo NFS da ONTAP.
- Você deseja executar tarefas menos comuns de configuração e manutenção, não configuração básica de NFS.
- Você deseja usar a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Entenda o acesso a arquivos nas

Namespaces e pontos de junção

Visão geral de namespaces e pontos de junção

Um nas *namespace* é um agrupamento lógico de volumes Unidos em *pontos de junção* para criar uma única hierarquia de sistema de arquivos. Um cliente com permissões suficientes pode acessar arquivos no namespace sem especificar a localização dos arquivos no armazenamento. Os volumes Junctioned podem residir em qualquer lugar do cluster.

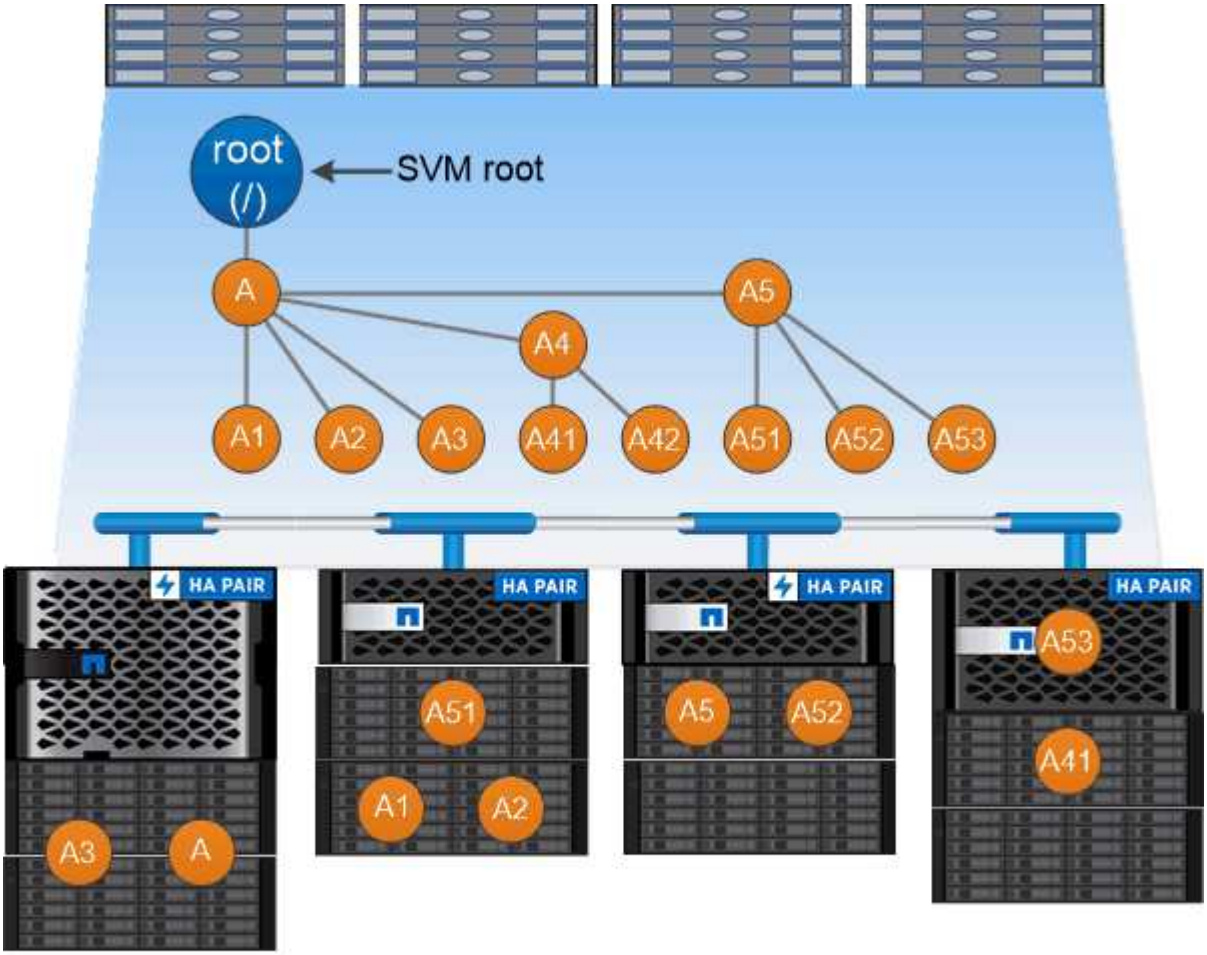
Em vez de montar cada volume contendo um arquivo de interesse, os clientes nas montam um NFS *export* ou acessam um SMB *share.* a exportação ou compartilhamento representa todo o namespace ou um local intermediário dentro do namespace. O cliente acessa apenas os volumes montados abaixo do seu ponto de acesso.

Você pode adicionar volumes ao namespace conforme necessário. Você pode criar pontos de junção diretamente abaixo de uma junção de volume pai ou em um diretório dentro de um volume. Um caminho para

uma junção de volume para um volume chamado "'vol3" pode ser `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou mesmo `/dir1/dir2/vol3`. O caminho é chamado de *caminho de junção.*

Cada SVM tem um namespace único. O volume raiz da SVM é o ponto de entrada para a hierarquia de namespace.

Para garantir que os dados permaneçam disponíveis no caso de uma interrupção do nó ou failover, você deve criar uma cópia de *load-sharing mirror* para o volume raiz da SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Quais são as arquiteturas típicas de namespace nas

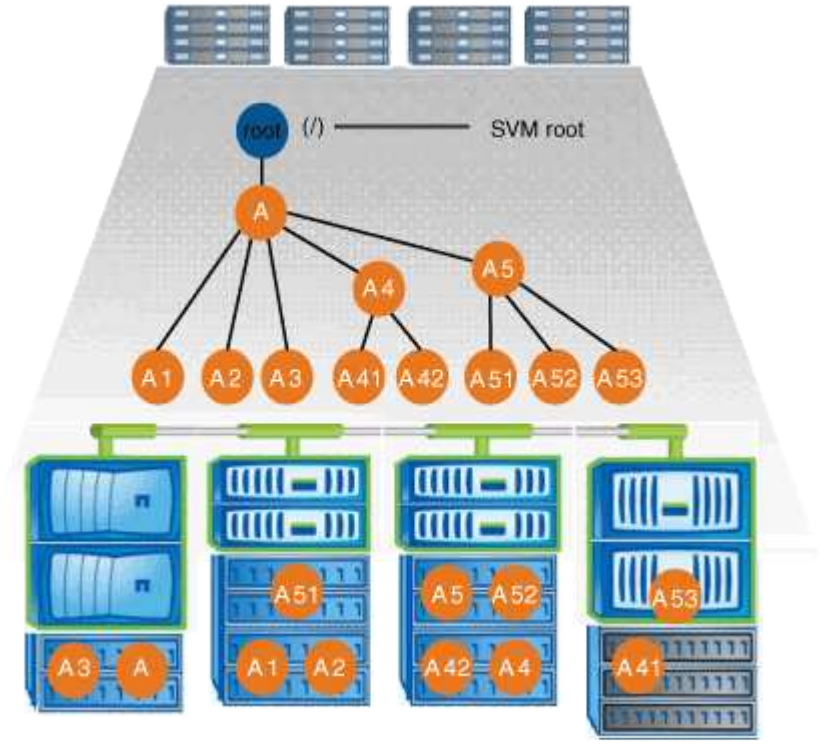
Há várias arquiteturas típicas de namespace nas que você pode usar ao criar seu espaço de nomes SVM. Você pode escolher a arquitetura de namespace que corresponde às necessidades da sua empresa e do fluxo de trabalho.

A parte superior do namespace é sempre o volume raiz, que é representado por uma barra (/). A arquitetura de namespace sob a raiz se enquadra em três categorias básicas:

- Uma única árvore ramificada, com apenas uma única junção para a raiz do namespace
- Várias árvores ramificadas, com vários pontos de junção para a raiz do namespace
- Vários volumes independentes, cada um com um ponto de junção separado para a raiz do espaço de nomes

Namespace com árvore ramificada única

Uma arquitetura com uma única árvore ramificada tem um único ponto de inserção para a raiz do namespace SVM. O ponto de inserção único pode ser um volume juntado ou um diretório sob a raiz. Todos os outros volumes são montados em pontos de junção abaixo do ponto de inserção único (que pode ser um volume ou um diretório).

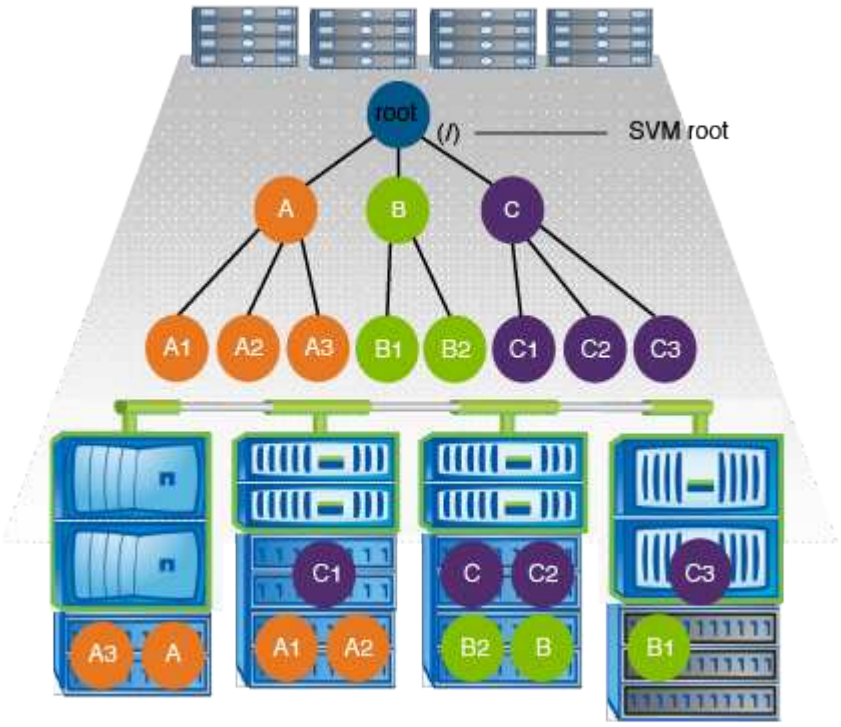


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde todos os volumes são juntados abaixo do ponto de inserção único, que é um diretório chamado "data":

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     corp1       true     /data/dir1/corp1       RW_volume
vs1     corp2       true     /data/dir1/corp2       RW_volume
vs1     data1       true     /data/data1            RW_volume
vs1     eng1        true     /data/data1/eng1       RW_volume
vs1     eng2        true     /data/data1/eng2       RW_volume
vs1     sales       true     /data/data1/sales      RW_volume
vs1     vol1        true     /data/vol1             RW_volume
vs1     vol2        true     /data/vol2             RW_volume
vs1     vol3        true     /data/vol3             RW_volume
vs1     vs1_root    -        /                      -
```

Namespace com várias árvores ramificadas

Uma arquitetura com várias árvores ramificadas tem vários pontos de inserção na raiz do namespace SVM. Os pontos de inserção podem ser volumes juntados ou diretórios abaixo da raiz. Todos os outros volumes são montados em pontos de junção abaixo dos pontos de inserção (que podem ser volumes ou diretórios).

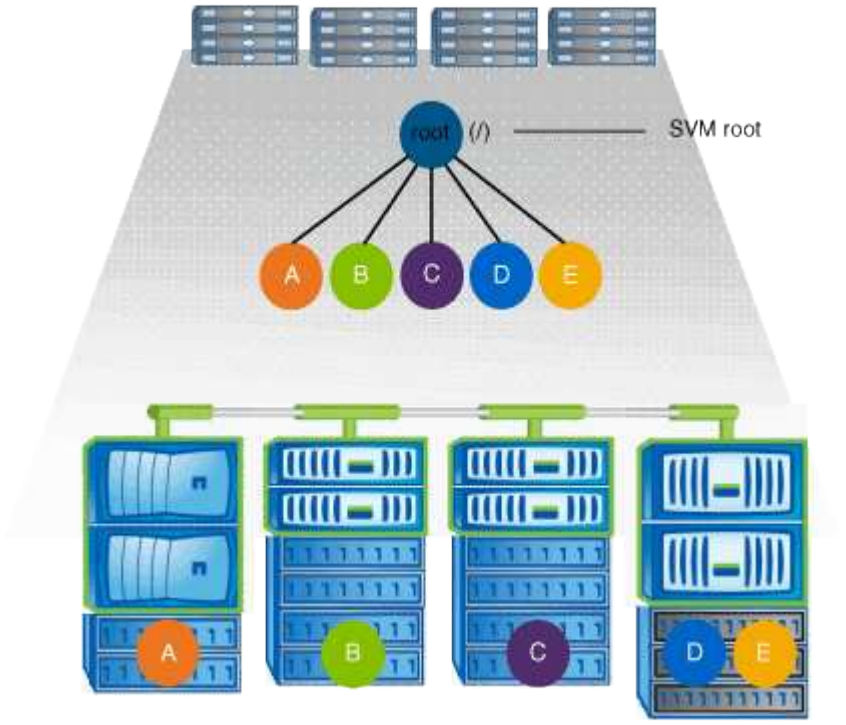


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há três pontos de inserção para o volume raiz do SVM. Dois pontos de inserção são diretórios denominados "data" e "projetos". Um ponto de inserção é um volume juntado chamado "audit":

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

Namespace com vários volumes autônomos

Em uma arquitetura com volumes autônomos, cada volume tem um ponto de inserção para a raiz do namespace SVM. No entanto, o volume não é juntado abaixo de outro volume. Cada volume tem um caminho exclusivo e é juntado diretamente abaixo da raiz ou é juntado sob um diretório abaixo da raiz.



Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há cinco pontos de inserção para o volume raiz do SVM, com cada ponto de inserção representando um caminho para um volume.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

Como o ONTAP controla o acesso aos arquivos

Como o ONTAP controla o acesso aos arquivos

O ONTAP controla o acesso aos arquivos de acordo com as restrições baseadas em autenticação e em arquivo especificadas.

Quando um cliente se coneta ao sistema de armazenamento para acessar arquivos, o ONTAP tem que executar duas tarefas:

- Autenticação

  O ONTAP tem que autenticar o cliente verificando a identidade com uma fonte confiável. Além disso, o tipo de autenticação do cliente é um método que pode ser usado para determinar se um cliente pode acessar dados ao configurar políticas de exportação (opcional para CIFS).

- Autorização

  O ONTAP tem que autorizar o usuário comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório e determinando que tipo de acesso, se houver, a fornecer.

Para gerenciar adequadamente o controle de acesso a arquivos, o ONTAP deve se comunicar com serviços externos, como NIS, LDAP e servidores do ative Directory. A configuração de um sistema de storage para acesso a arquivos usando CIFS ou NFS requer a configuração dos serviços apropriados, dependendo do seu ambiente no ONTAP.

Restrições baseadas em autenticação

Com restrições baseadas em autenticação, você pode especificar quais máquinas cliente e quais usuários podem se conetar à máquina virtual de armazenamento (SVM).

O ONTAP suporta autenticação Kerberos de servidores UNIX e Windows.

Restrições baseadas em arquivos

O ONTAP avalia três níveis de segurança para determinar se uma entidade está autorizada a executar uma ação solicitada em arquivos e diretórios localizados em um SVM. O acesso é determinado pelas permissões efetivas após a avaliação dos três níveis de segurança.

Qualquer objeto de armazenamento pode conter até três tipos de camadas de segurança:

- Segurança de exportação (NFS) e compartilhamento (SMB)

  A segurança de exportação e compartilhamento se aplica ao acesso do cliente a uma determinada exportação NFS ou compartilhamento SMB. Os usuários com Privileges administrativo podem gerenciar a segurança de exportação e compartilhamento a partir de clientes SMB e NFS.

- Segurança de arquivo e diretório do Access Guard no nível de armazenamento

  A segurança do Access Guard no nível de storage se aplica ao acesso de clientes SMB e NFS aos volumes SVM. Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

  > Se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança do Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX).

- Segurança nativa em nível de arquivo NTFS, UNIX e NFSv4

  A segurança de nível de arquivo nativo existe no arquivo ou diretório que representa o objeto de storage. Você pode definir a segurança no nível do arquivo de um cliente. As permissões de arquivo são efetivas independentemente de SMB ou NFS serem usados para acessar os dados.

Como o ONTAP lida com a autenticação de cliente NFS

Como o ONTAP lida com a visão geral da autenticação do cliente NFS

Os clientes NFS devem ser devidamente autenticados antes de poderem acessar os dados no SVM. O ONTAP autentica os clientes verificando suas credenciais UNIX em relação aos serviços de nome que você configura.

Quando um cliente NFS se coneta ao SVM, o ONTAP obtém as credenciais UNIX para o usuário verificando diferentes serviços de nome, dependendo da configuração dos serviços de nome do SVM. O ONTAP pode verificar credenciais para contas UNIX locais, domínios NIS e domínios LDAP. Pelo menos um deles deve ser configurado para que o ONTAP possa autenticar com êxito o usuário. Você pode especificar vários serviços de nomes e a ordem em que o ONTAP os procura.

Em um ambiente NFS puro com estilos de segurança de volume UNIX, essa configuração é suficiente para autenticar e fornecer o acesso de arquivo adequado para um usuário conetado a partir de um cliente NFS.

Se você estiver usando estilos de segurança de volume misto, NTFS ou unificado, o ONTAP deve obter um nome de usuário SMB para o usuário UNIX para autenticação com um controlador de domínio do Windows. Isso pode acontecer mapeando usuários individuais usando contas UNIX locais ou domínios LDAP, ou usando um usuário SMB padrão em vez disso. Você pode especificar quais serviços de nome o ONTAP pesquisa em qual ordem ou especificar um usuário SMB padrão.

Como o ONTAP usa os serviços de nomes

O ONTAP usa serviços de nome para obter informações sobre usuários e clientes. O

ONTAP usa essas informações para autenticar usuários acessando dados ou administrando o sistema de storage e mapear credenciais de usuário em um ambiente misto.

Ao configurar o sistema de storage, você deve especificar quais serviços de nome deseja que o ONTAP use para obter credenciais de usuário para autenticação. O ONTAP oferece suporte aos seguintes serviços de nomes:

- Utilizadores locais (ficheiro)
- Domínios NIS externos (NIS)
- Domínios LDAP externos (LDAP)

Você usa a `vserver services name-service ns-switch` família de comandos para configurar SVMs com as fontes para procurar informações de rede e a ordem na qual pesquisá-las. Esses comandos fornecem a funcionalidade equivalente do `/etc/nsswitch.conf` arquivo em sistemas UNIX.

Quando um cliente NFS se coneta ao SVM, o ONTAP verifica os serviços de nome especificados para obter as credenciais UNIX do usuário. Se os serviços de nome estiverem configurados corretamente e o ONTAP puder obter as credenciais UNIX, o ONTAP autentica o usuário com êxito.

Em um ambiente com estilos de segurança mistos, o ONTAP pode ter que mapear as credenciais do usuário. Você deve configurar os serviços de nome adequadamente para o seu ambiente para permitir que o ONTAP mapeie corretamente as credenciais do usuário.

O ONTAP também usa serviços de nomes para autenticar contas de administrador da SVM. Você deve ter isso em mente ao configurar ou modificar o switch do serviço de nomes para evitar desabilitar acidentalmente a autenticação para contas de administrador SVM. Para obter mais informações sobre usuários de administração do SVM, "Autenticação de administrador e RBAC"consulte .

Como o ONTAP concede acesso a arquivos SMB de clientes NFS

O ONTAP usa a semântica de segurança do sistema de arquivos do Windows NT (NTFS) para determinar se um usuário UNIX, em um cliente NFS, tem acesso a um arquivo com permissões NTFS.

O ONTAP faz isso convertendo o ID de usuário UNIX do usuário (UID) em uma credencial SMB e, em seguida, usando a credencial SMB para verificar se o usuário tem direitos de acesso ao arquivo. Uma credencial SMB consiste em um SID (Identificador de Segurança primário), geralmente o nome de usuário do Windows do usuário e um ou mais SIDs de grupo que correspondem aos grupos do Windows dos quais o usuário é membro.

O Time ONTAP leva a conversão do UID UNIX em uma credencial SMB pode ser de dezenas de milissegundos a centenas de milissegundos, porque o processo envolve entrar em Contato com um controlador de domínio. O ONTAP mapeia o UID para a credencial SMB e insere o mapeamento em um cache de credenciais para reduzir o tempo de verificação causado pela conversão.

Como funciona o cache de credenciais NFS

Quando um usuário NFS solicita acesso às exportações de NFS no sistema de storage, o ONTAP deve recuperar as credenciais de usuário de servidores de nomes externos ou de arquivos locais para autenticar o usuário. Em seguida, o ONTAP armazena essas credenciais em um cache interno de credenciais para referência posterior. Entender

como os caches de credenciais NFS funcionam permite que você lide com possíveis problemas de desempenho e acesso.

Sem o cache de credenciais, o ONTAP teria que consultar serviços de nomes sempre que um usuário NFS solicitou acesso. Em um sistema de armazenamento ocupado que é acessado por muitos usuários, isso pode rapidamente levar a sérios problemas de desempenho, causando atrasos indesejados ou até mesmo negações ao acesso do cliente NFS.

Com o cache de credenciais, o ONTAP recupera as credenciais do usuário e as armazena por um período predeterminado de tempo para acesso rápido e fácil caso o cliente NFS envie outra solicitação. Este método oferece as seguintes vantagens:

- Ele facilita a carga no sistema de armazenamento, manipulando menos solicitações para servidores de nomes externos (como NIS ou LDAP).
- Ele facilita a carga em servidores de nomes externos, enviando menos solicitações para eles.
- Ele acelera o acesso do usuário eliminando o tempo de espera para obter credenciais de fontes externas antes que o usuário possa ser autenticado.

O ONTAP armazena credenciais positivas e negativas no cache de credenciais. Credenciais positivas significa que o usuário foi autenticado e recebeu acesso. Credenciais negativas significa que o usuário não foi autenticado e foi negado o acesso.

Por padrão, o ONTAP armazena credenciais positivas por 24 horas; ou seja, após a autenticação inicial de um usuário, o ONTAP usa as credenciais em cache para quaisquer solicitações de acesso por esse usuário por 24 horas. Se o usuário solicitar acesso após 24 horas, o ciclo será iniciado novamente: O ONTAP descarta as credenciais armazenadas em cache e obtém as credenciais novamente a partir da fonte de serviço de nome apropriada. Se as credenciais tiverem sido alteradas no servidor de nomes durante as 24 horas anteriores, o ONTAP armazena em cache as credenciais atualizadas para uso nas próximas 24 horas.

Por padrão, o ONTAP armazena credenciais negativas por duas horas; ou seja, depois de inicialmente negar acesso a um usuário, o ONTAP continua negando quaisquer solicitações de acesso por esse usuário por duas horas. Se o usuário solicitar acesso após 2 horas, o ciclo será iniciado novamente: O ONTAP obtém as credenciais novamente da fonte de serviço de nome apropriada. Se as credenciais tiverem sido alteradas no servidor de nomes durante as duas horas anteriores, o ONTAP armazena em cache as credenciais atualizadas para uso nas próximas duas horas.

Crie e gerencie volumes de dados em namespaces nas

Crie volumes de dados com pontos de junção especificados

Pode especificar o ponto de junção quando cria um volume de dados. O volume resultante é montado automaticamente no ponto de junção e está imediatamente disponível para configurar para acesso nas.

Antes de começar

- O agregado no qual você deseja criar o volume já deve existir.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Os seguintes carateres não podem ser usados no caminho de junção: * *

Além disso, o comprimento do caminho de junção não pode ter mais de 255 carateres.

Passos

1. Crie o volume com um ponto de junção:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   O caminho de junção deve começar com a raiz (/) e pode conter diretórios e volumes juntados. O caminho de junção não precisa conter o nome do volume. Os caminhos de junção são independentes do nome do volume.

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados criado. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   O caminho de junção é insensível a maiúsculas e minúsculas; `/ENG` é o mesmo que `/eng`. Se você criar um compartilhamento CIFS, o Windows tratará o caminho de junção como se ele fosse sensível a maiúsculas e minúsculas. Por exemplo, se a junção for `/ENG`, o caminho de um compartilhamento SMB deve começar com `/ENG`, não `/eng`.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado:

   `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Crie volumes de dados sem especificar pontos de junção

Você pode criar um volume de dados sem especificar um ponto de junção. O volume resultante não é montado automaticamente e não está disponível para configuração para acesso nas. É necessário montar o volume antes de configurar compartilhamentos SMB ou exportações NFS para esse volume.

Antes de começar

- O agregado no qual você deseja criar o volume já deve existir.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume sem um ponto de junção usando o seguinte comando:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado sem um ponto de junção:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Exemplo

O exemplo a seguir cria um volume chamado "vendas" localizado no SVM VS1 que não está montado em um ponto de junção:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Montar ou desmontar volumes existentes no namespace nas

Um volume deve ser montado no namespace nas antes de poder configurar o acesso do cliente nas aos dados contidos nos volumes de máquina virtual de storage (SVM). Você pode montar um volume em um ponto de junção se ele não estiver montado no momento. Você também pode desmontar volumes.

Sobre esta tarefa

Se você desmontar e colocar um volume off-line, todos os dados dentro do ponto de junção, incluindo dados em volumes com pontos de junção contidos no namespace do volume não montado, ficarão inacessíveis para clientes nas.

> Para interromper o acesso de cliente nas a um volume, não é suficiente simplesmente desmontar o volume. Você deve colocar o volume off-line ou tomar outras medidas para garantir que os caches de manipulação de arquivos do lado do cliente sejam invalidados. Para obter mais informações, consulte o seguinte artigo da base de dados de Conhecimento:
>
> "Os clientes NFSv3 ainda têm acesso a um volume depois de serem removidos do namespace no ONTAP"

Quando você desmontar e off-line um volume, os dados dentro do volume não são perdidos. Além disso, políticas de exportação de volume existentes e compartilhamentos SMB criados no volume ou em diretórios e pontos de junção dentro do volume não montado são retidos. Se você remontar o volume não montado, os clientes nas poderão acessar os dados contidos no volume usando políticas de exportação e compartilhamentos SMB existentes.

Passos

1. Execute a ação desejada:

Se você quiser…	Digite os comandos…
Monte um volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

Se você quiser…	Digite os comandos…

Desmontar um volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Verifique se o volume está no estado de montagem desejado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemplos

O exemplo a seguir monta um volume chamado "vendas" localizado na SVM "VS1" no ponto de junção ""/vendas":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

O exemplo a seguir desmonta e fica offline um volume chamado "data" localizado na SVM ""VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Apresentar informações sobre a montagem do volume e o ponto de junção

Você pode exibir informações sobre volumes montados para máquinas virtuais de armazenamento (SVMs) e os pontos de junção para os quais os volumes são montados.

Você também pode determinar quais volumes não estão montados em um ponto de junção. Use essas informações para entender e gerenciar seu namespace SVM.

Passo

1. Execute a ação desejada:

Se você quiser exibir…	Digite o comando…
Informações resumidas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -junction`
Informações detalhadas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Informações específicas sobre volumes montados e não montados no SVM	a. Se necessário, você pode exibir campos válidos para o `-fields` parâmetro usando o seguinte comando: `volume show -fields ?` b. Apresentar a informação pretendida utilizando o `-fields` parâmetro: `volume show -vserver vserver_name -fields fieldname,…`

Exemplos

O exemplo a seguir exibe um resumo dos volumes montados e não montados no SVM VS1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

O exemplo a seguir exibe informações sobre campos especificados para volumes localizados no SVM VS2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Estilos de segurança e seus efeitos

Existem quatro estilos de segurança diferentes: UNIX, NTFS, misto e unificado. Cada estilo de segurança tem um efeito diferente sobre como as permissões são tratadas para os dados. Você deve entender os diferentes efeitos para garantir que você selecione o estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar dados. Os estilos de segurança determinam apenas o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e que tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa estilo de segurança UNIX, os clientes SMB ainda podem acessar dados (desde que autentiquem e autorizem adequadamente) devido à natureza multiprotocolo do ONTAP. No entanto, o ONTAP usa permissões UNIX que somente clientes UNIX podem modificar usando ferramentas nativas.

Estilo de segurança	Clientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Clientes que podem acessar arquivos
UNIX	NFS	NFSv3 bits de modo	UNIX	NFS e SMB
		ACLs NFSv4.x		
NTFS	SMB	ACLs NTFS	NTFS	
Misto	NFS ou SMB	NFSv3 bits de modo	UNIX	
		NFSv4.ACLs		
		ACLs NTFS	NTFS	
Unificado (somente para volumes infinitos, no ONTAP 9.4 e versões anteriores).	NFS ou SMB	NFSv3 bits de modo	UNIX	
		ACLs NFSv4,1		
		ACLs NTFS	NTFS	

Os volumes FlexVol suportam estilos de segurança UNIX, NTFS e mistos. Quando o estilo de segurança é misto ou unificado, as permissões efetivas dependem do tipo de cliente que modificou as permissões pela última vez porque os usuários definem o estilo de segurança individualmente. Se o último cliente que modificou permissões fosse um cliente NFSv3, as permissões são bits do modo UNIX NFSv3. Se o último cliente foi um cliente NFSv4, as permissões são NFSv4 ACLs. Se o último cliente foi um cliente SMB, as permissões são ACLs do Windows NTFS.

O estilo de segurança unificado só está disponível com volumes infinitos, que não são mais suportados no ONTAP 9.5 e versões posteriores. Para obter mais informações, Visão geral do gerenciamento do FlexGroup volumesconsulte .

A partir do ONTAP 9.2, o `show-effective-permissions` parâmetro para o `vserver security file-directory` comando permite exibir permissões efetivas concedidas a um usuário Windows ou UNIX no caminho especificado de arquivo ou pasta. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo.

> O ONTAP define inicialmente algumas permissões de arquivo padrão. Por padrão, o estilo de segurança eficaz em todos os dados em UNIX, volumes mistos e de estilo de segurança unificado é UNIX e o tipo de permissões efetivas é bits de modo UNIX (0755 a menos que especificado de outra forma) até ser configurado por um cliente como permitido pelo estilo de segurança padrão. Por padrão, o estilo de segurança eficaz em todos os dados em volumes de estilo de segurança NTFS é NTFS e tem uma ACL que permite o controle total para todos.

Onde e quando definir estilos de segurança

Os estilos de segurança podem ser definidos em volumes FlexVol (raiz ou volumes de dados) e qtrees. Os estilos de segurança podem ser definidos manualmente no momento da criação, herdados automaticamente ou alterados posteriormente.

Decida qual estilo de segurança usar em SVMs

Para ajudá-lo a decidir qual estilo de segurança usar em um volume, você deve considerar dois fatores. O fator principal é o tipo de administrador que gerencia o sistema

de arquivos. O fator secundário é o tipo de usuário ou serviço que acessa os dados no volume.

Ao configurar o estilo de segurança em um volume, você deve considerar as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança e evite problemas com o gerenciamento de permissões. As seguintes considerações podem ajudá-lo a decidir:

Estilo de segurança	Escolha se…
UNIX	• O sistema de arquivos é gerenciado por um administrador UNIX. • A maioria dos usuários são clientes NFS. • Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	• O sistema de arquivos é gerenciado por um administrador do Windows. • A maioria dos usuários são clientes SMB. • Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	• O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Como a herança de estilo de segurança funciona

Se você não especificar o estilo de segurança ao criar um novo FlexVol volume ou uma qtree, ele herdará seu estilo de segurança de maneiras diferentes.

Os estilos de segurança são herdados da seguinte maneira:

- Um FlexVol volume herda o estilo de segurança do volume raiz do SVM.
- Uma qtree herda o estilo de segurança do seu que contém FlexVol volume.
- Um arquivo ou diretório herda o estilo de segurança dele contendo FlexVol volume ou qtree.

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

  Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

  Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Configurar estilos de segurança em volumes raiz do SVM

Você configura o estilo de segurança do volume raiz da máquina virtual de storage (SVM) para determinar o tipo de permissões usado para dados no volume raiz do SVM.

Passos

1. Use o `vserver create` comando com o `-rootvolume-security-style` parâmetro para definir o estilo de segurança.

   As opções possíveis para o estilo de segurança do volume raiz são `unix`, `ntfs` ou `mixed`.

2. Exiba e verifique a configuração, incluindo o estilo de segurança do volume raiz do SVM criado:

   `vserver show -vserver` *`vserver_name`*

Configurar estilos de segurança no FlexVol volumes

Você configura o estilo de segurança do FlexVol volume para determinar o tipo de permissões usadas para dados nos volumes do FlexVol da máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se o FlexVol volume…	Use o comando…
Ainda não existe	`volume create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança do FlexVol volume são `unix`, `ntfs` ou `mixed`.

   Se você não especificar um estilo de segurança ao criar um FlexVol volume, o volume herdará o estilo de segurança do volume raiz.

   Para obter mais informações sobre os `volume create` comandos ou `volume modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança do FlexVol volume criado, digite o seguinte comando:

   ```
   volume show -volume volume_name -instance
   ```

Configurar estilos de segurança no qtrees

Você configura o estilo de segurança do volume de qtree para determinar o tipo de permissões usadas para dados no qtrees.

Passos

1. Execute uma das seguintes ações:

Se a qtree…	Use o comando…
Ainda não existe	`volume qtree create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume qtree modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança de qtree são `unix`, `ntfs`, ou `mixed`.

   Se você não especificar um estilo de segurança ao criar uma qtree, o estilo de segurança padrão será

`mixed`.

Para obter mais informações sobre os `volume qtree create` comandos ou `volume qtree modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança da qtree que você criou, digite o seguinte comando: `volume qtree show -qtree qtree_name -instance`

Configurar o acesso a arquivos usando NFS

Configure o acesso a arquivos usando a visão geral do NFS

Você deve concluir várias etapas para permitir que os clientes acessem arquivos em máquinas virtuais de armazenamento (SVMs) usando NFS. Existem algumas etapas adicionais que são opcionais, dependendo da configuração atual do seu ambiente.

Para que os clientes possam acessar arquivos em SVMs usando NFS, você deve concluir as seguintes tarefas:

1. Habilite o protocolo NFS na SVM.

   Você precisa configurar o SVM para permitir acesso a dados de clientes em NFS.

2. Criar um servidor NFS no SVM.

   Um servidor NFS é uma entidade lógica no SVM que permite que o SVM forneça arquivos em NFS. Você deve criar o servidor NFS e especificar as versões do protocolo NFS que deseja permitir.

3. Configurar políticas de exportação no SVM.

   Você deve configurar políticas de exportação para tornar os volumes e qtrees disponíveis para os clientes.

4. Configure o servidor NFS com a segurança adequada e outras configurações, dependendo da rede e do ambiente de armazenamento.

   Esta etapa pode incluir a configuração Kerberos, "NFS em TLS", LDAP, NIS, mapeamentos de nomes e usuários locais.

Proteja o acesso NFS usando políticas de exportação

Como as políticas de exportação controlam o acesso do cliente a volumes ou qtrees

As políticas de exportação contêm uma ou mais *regras de exportação* que processam cada solicitação de acesso de cliente. O resultado do processo determina se o cliente é negado ou concedido acesso e que nível de acesso. Uma política de exportação com regras de exportação deve existir na máquina virtual de storage (SVM) para que os clientes acessem os dados.

Você associa exatamente uma política de exportação a cada volume ou qtree para configurar o acesso do cliente ao volume ou qtree. O SVM pode conter várias políticas de exportação. Isso permite que você faça o seguinte para SVMs com vários volumes ou qtrees:

- Atribua diferentes políticas de exportação a cada volume ou qtree do SVM para controle de acesso de cliente individual a cada volume ou qtree no SVM.
- Atribua a mesma política de exportação a vários volumes ou qtrees do SVM para controle de acesso de cliente idêntico sem ter que criar uma nova política de exportação para cada volume ou qtree.

Se um cliente fizer uma solicitação de acesso que não é permitida pela política de exportação aplicável, a solicitação falhará com uma mensagem de permissão negada. Se um cliente não corresponder a nenhuma regra na política de exportação, o acesso será negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados.

Você pode modificar uma política de exportação dinamicamente em um sistema executando o ONTAP.

Política de exportação padrão para SVMs

Cada SVM tem uma política de exportação padrão que não contém regras. Uma política de exportação com regras deve existir antes que os clientes possam acessar os dados no SVM. Cada FlexVol volume contido no SVM deve estar associado a uma política de exportação.

Ao criar um SVM, o sistema de storage cria automaticamente uma política de exportação padrão chamada `default` volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM. Como alternativa, você pode criar uma política de exportação personalizada com regras. Você pode modificar e renomear a política de exportação padrão, mas não pode excluir a política de exportação padrão.

Quando você cria um FlexVol volume que contém o SVM, o sistema de storage cria o volume e associa o volume à política de exportação padrão para o volume raiz do SVM. Por padrão, cada volume criado no SVM está associado à política de exportação padrão do volume raiz. Você pode usar a política de exportação padrão para todos os volumes contidos no SVM ou criar uma política de exportação exclusiva para cada volume. Você pode associar vários volumes à mesma política de exportação.

Como funcionam as regras de exportação

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente a um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente.

Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação. A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

Você pode configurar regras de exportação para determinar permissões de acesso do cliente usando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação, por exemplo, NFSv4 ou SMB.
- Um identificador de cliente, por exemplo, nome de host ou endereço IP.

  O tamanho máximo para o `-clientmatch` campo é de 4096 carateres.

- O tipo de segurança usado pelo cliente para autenticar, por exemplo, Kerberos v5, NTLM ou AUTH_SYS.

Se uma regra especificar vários critérios, o cliente deve corresponder a todos eles para que a regra seja aplicada.

> A partir do ONTAP 9.3, você pode habilitar a verificação de configuração de política de exportação como uma tarefa em segundo plano que Registra quaisquer violações de regras em uma lista de regras de erro. Os `vserver export-policy config-checker` comandos invocam o verificador e exibem resultados, que podem ser usados para verificar sua configuração e excluir regras errôneas da política.
>
> Os comandos apenas validam a configuração de exportação para nomes de host, netgroups e usuários anônimos.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv3 e o cliente tem o endereço IP 10,1.17,37.

Mesmo que o protocolo de acesso do cliente corresponda, o endereço IP do cliente está em uma sub-rede diferente da especificada na regra de exportação. Portanto, a correspondência do cliente falha e esta regra não se aplica a este cliente.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv4 e o cliente tem o endereço IP 10,1.16,54.

O protocolo de acesso do cliente corresponde e o endereço IP do cliente está na sub-rede especificada. Portanto, a correspondência do cliente é bem-sucedida e esta regra se aplica a este cliente. O cliente obtém acesso de leitura e gravação independentemente do seu tipo de segurança.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`

- `-rorule any`
- `-rwrule krb5,ntlm`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. Portanto, ambos os clientes recebem acesso somente leitura. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

Gerencie clientes com um tipo de segurança não listado

Quando um cliente se apresenta com um tipo de segurança que não está listado em um parâmetro de acesso de uma regra de exportação, você tem a opção de negar acesso ao cliente ou mapeá-lo para o ID de usuário anônimo usando a opção `none` no parâmetro de acesso.

Um cliente pode apresentar-se com um tipo de segurança que não está listado em um parâmetro de acesso porque foi autenticado com um tipo de segurança diferente ou não foi autenticado de todo (tipo de segurança AUTH_NONE). Por padrão, o cliente é automaticamente negado o acesso a esse nível. No entanto, você pode adicionar a opção `none` ao parâmetro Access. Como resultado, os clientes com um estilo de segurança não listado são mapeados para o ID de usuário anônimo. O `-anon` parâmetro determina qual ID de usuário é atribuído a esses clientes. O ID de usuário especificado para o `-anon` parâmetro deve ser um usuário válido que esteja configurado com permissões que você considere apropriadas para o usuário anônimo.

Valores válidos para o `-anon` intervalo de parâmetros `0` de a `65535`.

ID de utilizador atribuída a `-anon`	**Processamento resultante de solicitações de acesso do cliente**
`0 - 65533`	A solicitação de acesso do cliente é mapeada para o ID de usuário anônimo e obtém acesso dependendo das permissões configuradas para esse usuário.
`65534`	A solicitação de acesso do cliente é mapeada para o usuário ninguém e obtém acesso dependendo das permissões configuradas para esse usuário. Este é o padrão.
`65535`	A solicitação de acesso de qualquer cliente é negada quando mapeada para essa ID e o cliente se apresenta com o tipo de segurança AUTH_NONE. A solicitação de acesso de clientes com ID de usuário 0 é negada quando mapeada para essa ID e o cliente se apresenta com qualquer outro tipo de segurança.

Ao usar a opção `none`, é importante lembrar que o parâmetro somente leitura é processado primeiro. Considere as seguintes diretrizes ao configurar regras de exportação para clientes com tipos de segurança não listados:

Somente leitura inclui `none`	**A leitura-gravação inclui** `none`	**Acesso resultante para clientes com tipos de segurança não listados**
Não	Não	Negado
Não	Sim	Negado porque somente leitura é processada primeiro
Sim	Não	Somente leitura como anônima
Sim	Sim	Leia-escreva como anônimo

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (ou seja, o tipo de segurança AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a clientes com seu próprio ID de usuário autenticado com AUTH_SYS. O parâmetro somente leitura permite o acesso somente leitura como usuário anônimo com ID de usuário 70 para clientes autenticados usando qualquer outro tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação a qualquer tipo de segurança, mas neste caso só se aplica a clientes já filtrados pela regra somente leitura.

Portanto, os clientes nº 1 e nº 3 recebem acesso de leitura e gravação apenas como usuário anônimo com ID de usuário 70. O cliente nº 2 obtém acesso de leitura e gravação com seu próprio ID de usuário.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (ou seja, o tipo de segurança AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a clientes com seu próprio ID de usuário autenticado com AUTH_SYS. O parâmetro somente leitura permite o acesso somente leitura como usuário anônimo com ID de usuário 70 para clientes autenticados usando qualquer outro tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação somente como usuário anônimo.

Portanto, o cliente nº 1 e o cliente nº 3 recebem acesso de leitura e gravação somente como usuário anônimo com ID de usuário 70. O cliente nº 2 obtém acesso somente leitura com seu próprio ID de usuário, mas é negado o acesso de leitura e gravação.

Como os tipos de segurança determinam os níveis de acesso do cliente

O tipo de segurança com o qual o cliente autenticou desempenha um papel especial nas regras de exportação. Você deve entender como o tipo de segurança determina os níveis de acesso que o cliente obtém a um volume ou qtree.

Os três níveis de acesso possíveis são os seguintes:

1. Somente leitura
2. Leitura-gravação
3. Superusuário (para clientes com ID de usuário 0)

Como o nível de acesso por tipo de segurança é avaliado nesta ordem, você deve observar as seguintes regras ao construir parâmetros de nível de acesso em regras de exportação:

Para um cliente obter nível de acesso…	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente…
Apenas de leitura normal do utilizador	Somente leitura (`-rorule`)
Leitura-escrita normal do utilizador	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`)
Somente leitura do superusuário	Apenas leitura (`-rorule`) e. `-superuser`

Para um cliente obter nível de acesso…	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente…
Leitura-gravação do superusuário	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`) e. `-superuser`

Os seguintes são tipos de segurança válidos para cada um destes três parâmetros de acesso:

- `any`
- `none`
- `never`

  Este tipo de segurança não é válido para utilização com o `-superuser` parâmetro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Ao combinar o tipo de segurança de um cliente com cada um dos três parâmetros de acesso, há três resultados possíveis:

Se o tipo de segurança do cliente…	Então o cliente…
Corresponde ao especificado no parâmetro Access.	Obtém acesso para esse nível com seu próprio ID de usuário.
Não corresponde ao especificado, mas o parâmetro Access inclui a opção `none`.	Obtém acesso para esse nível, mas como o usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro.
Não corresponde ao especificado e o parâmetro Access não inclui a opção `none`.	Não obtém acesso para esse nível. Isso não se aplica ao `-superuser` parâmetro porque ele sempre inclui `none` mesmo quando não especificado.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação a clientes com sua própria ID de usuário autenticado com AUTH_SYS ou Kerberos v5. O parâmetro superuser permite o acesso do superusuário a clientes com ID de usuário 0 autenticado com Kerberos v5.

Portanto, o cliente nº 1 obtém acesso de leitura e gravação do superusuário porque ele corresponde aos três parâmetros de acesso. O cliente nº 2 obtém acesso de leitura e gravação, mas não acesso ao superusuário. O cliente nº 3 obtém acesso somente leitura, mas não acesso ao superusuário.

Gerenciar solicitações de acesso de superusuário

Ao configurar políticas de exportação, você precisa considerar o que deseja acontecer se o sistema de armazenamento receber uma solicitação de acesso de cliente com ID de usuário 0, ou seja, como superusuário, e configurar suas regras de exportação de acordo.

No mundo UNIX, um usuário com o ID de usuário 0 é conhecido como superusuário, normalmente chamado de root, que tem direitos de acesso ilimitados em um sistema. O uso do superusuário Privileges pode ser perigoso por várias razões, incluindo a violação do sistema e da segurança de dados.

Por padrão, o ONTAP mapeia os clientes que apresentam com ID de usuário 0 para o usuário anônimo. No entanto, você pode especificar o `- superuser` parâmetro em regras de exportação para determinar como lidar com clientes que apresentam com ID de usuário 0, dependendo do seu tipo de segurança. A seguir estão as opções válidas para o `-superuser` parâmetro:

- `any`
- `none`

  Esta é a configuração padrão se você não especificar o `-superuser` parâmetro.

- `krb5`
- `ntlm`
- `sys`

Há duas maneiras diferentes de como os clientes que apresentam com ID de usuário 0 são manipulados, dependendo da `-superuser` configuração do parâmetro:

Se o `-superuser` parâmetro e o tipo de segurança do cliente…	Então o cliente…
Correspondência	Obtém acesso de superusuário com ID de usuário 0.

Se o `-superuser` parâmetro e o tipo de segurança do cliente…	Então o cliente…
Não corresponder	Obtém acesso como usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro e suas permissões atribuídas. Isso é independentemente de o parâmetro somente leitura ou leitura-gravação especificar a opção `none`.

Se um cliente apresentar com ID de usuário 0 para acessar um volume com estilo de segurança NTFS e o `-superuser` parâmetro estiver definido como `none`, o ONTAP usará o mapeamento de nomes para o usuário anônimo obter as credenciais adequadas.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 746, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar.

O cliente nº 2 não obtém acesso ao superusuário. Em vez disso, ele é mapeado para anônimo porque o `-superuser` parâmetro não é especificado. Isto significa que o padrão é `none` e mapeia automaticamente a ID do usuário 0 para anônimo. O cliente nº 2 também só obtém acesso somente leitura porque seu tipo de segurança não corresponde ao parâmetro de leitura-gravação.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

A regra de exportação permite o acesso do superusuário para clientes com ID de usuário 0. O cliente nº 1 obtém acesso ao superusuário porque corresponde ao ID do usuário e ao tipo de segurança para somente leitura e `-superuser` parâmetros. O cliente nº 2 não obtém acesso de leitura-escrita ou superusuário porque seu tipo de segurança não corresponde ao parâmetro de leitura-gravação ou ao `-superuser` parâmetro. Em vez disso, o cliente nº 2 é mapeado para o usuário anônimo, que neste caso tem o ID de usuário 0.

Como o ONTAP usa caches de política de exportação

Para melhorar o desempenho do sistema, o ONTAP usa caches locais para armazenar informações como nomes de host e grupos de rede. Isso permite que o ONTAP processe regras de política de exportação mais rapidamente do que recuperar as informações de fontes externas. Entender o que são os caches e o que eles fazem pode ajudá-lo a solucionar problemas de acesso ao cliente.

Você configura políticas de exportação para controlar o acesso do cliente às exportações NFS. Cada política de exportação contém regras e cada regra contém parâmetros que correspondem à regra aos clientes que solicitam acesso. Alguns desses parâmetros exigem que o ONTAP entre em Contato com uma fonte externa, como servidores DNS ou NIS, para resolver objetos como nomes de domínio, nomes de host ou netgroups.

Essas comunicações com fontes externas levam um pouco de tempo. Para aumentar o desempenho, o ONTAP reduz o tempo necessário para resolver objetos de regra de política de exportação armazenando informações localmente em cada nó em vários caches.

Nome do cache	Tipo de informação armazenada
Acesso	Mapeamentos de clientes para políticas de exportação correspondentes
Nome	Mapeamentos de nomes de usuário UNIX para IDs de usuário UNIX correspondentes
ID	Mapeamentos de IDs de usuário UNIX para IDs de usuário UNIX correspondentes e IDs de grupo UNIX estendidos
Host	Mapeamentos de nomes de host para endereços IP correspondentes

Nome do cache	Tipo de informação armazenada
Grupo de rede	Mapeamentos de netgroups para endereços IP correspondentes de membros
Showmount	Lista de diretórios exportados do namespace SVM

Se você alterar as informações nos servidores de nomes externos em seu ambiente depois que o ONTAP as recuperou e armazenou localmente, os caches agora podem conter informações desatualizadas. Embora o ONTAP atualize caches automaticamente após determinados períodos de tempo, os caches diferentes têm tempos e algoritmos diferentes de expiração e atualização.

Outro motivo possível para que os caches contenham informações desatualizadas é quando o ONTAP tenta atualizar informações em cache, mas encontra uma falha ao tentar se comunicar com servidores de nomes. Se isso acontecer, o ONTAP continuará a usar as informações atualmente armazenadas nos caches locais para evitar a interrupção do cliente.

Como resultado, as solicitações de acesso ao cliente que devem ser bem-sucedidas podem falhar e as solicitações de acesso ao cliente que devem falhar podem ser bem-sucedidas. Você pode exibir e lavar manualmente alguns dos caches de política de exportação ao solucionar problemas de acesso ao cliente.

Como o cache de acesso funciona

O ONTAP usa um cache de acesso para armazenar os resultados da avaliação de regras de política de exportação para operações de acesso do cliente para um volume ou qtree. Isso resulta em melhorias de desempenho porque as informações podem ser recuperadas muito mais rapidamente do cache de acesso do que passar pelo processo de avaliação de regras de política de exportação sempre que um cliente envia uma solicitação de e/S.

Sempre que um cliente NFS enviar uma solicitação de e/S para acessar dados em um volume ou qtree, o ONTAP deve avaliar cada solicitação de e/S para determinar se deve conceder ou negar a solicitação de e/S. Essa avaliação envolve verificar todas as regras de política de exportação da política de exportação associada ao volume ou qtree. Se o caminho para o volume ou qtree envolver cruzar um ou mais pontos de junção, isso pode exigir a realização desta verificação para várias políticas de exportação ao longo do caminho.

Observe que essa avaliação ocorre para cada solicitação de e/S enviada de um cliente NFS, como leitura, gravação, lista, cópia e outras operações, não apenas para solicitações de montagem inicial.

Depois que o ONTAP identificou as regras de política de exportação aplicáveis e decidiu se deseja permitir ou negar a solicitação, o ONTAP cria uma entrada no cache de acesso para armazenar essas informações.

Quando um cliente NFS envia uma solicitação de e/S, o ONTAP observa o endereço IP do cliente, a ID do SVM e a política de exportação associada ao volume ou qtree de destino e verifica primeiro a entrada correspondente no cache de acesso. Se existir uma entrada correspondente no cache de acesso, o ONTAP usará as informações armazenadas para permitir ou negar a solicitação de e/S. Se uma entrada correspondente não existir, o ONTAP passa pelo processo normal de avaliação de todas as regras de política aplicáveis, conforme explicado acima.

As entradas de cache de acesso que não são usadas ativamente não são atualizadas. Isso reduz a comunicação desnecessária e desperdiçada com o nome externo serve.

Recuperar as informações do cache de acesso é muito mais rápido do que passar por todo o processo de avaliação de regras de política de exportação para cada solicitação de e/S. Portanto, o uso do cache de acesso melhora significativamente o desempenho reduzindo a sobrecarga das verificações de acesso do cliente.

Como funcionam os parâmetros de cache de acesso

Vários parâmetros controlam os períodos de atualização para entradas no cache de acesso. Entender como esses parâmetros funcionam permite modificá-los para ajustar o cache de acesso e equilibrar o desempenho com o quão recente é a informação armazenada.

O cache de acesso armazena entradas que consistem em uma ou mais regras de exportação que se aplicam a clientes que tentam acessar volumes ou qtrees. Essas entradas são armazenadas por um determinado período de tempo antes de serem atualizadas. O tempo de atualização é determinado pelos parâmetros de cache de acesso e depende do tipo de entrada de cache de acesso.

Você pode especificar parâmetros de cache de acesso para SVMs individuais. Isso permite que os parâmetros sejam diferentes de acordo com os requisitos de acesso à SVM. As entradas de cache de acesso que não são usadas ativamente não são atualizadas, o que reduz a comunicação desnecessária e desperdiçada com servidores de nomes externos.

Acesse o tipo de entrada de cache	Descrição	Período de atualização em segundos
Entradas positivas	Acesse entradas de cache que não resultaram na negação de acesso aos clientes.	Mínimo: 300 Máximo: 86.400 Padrão: 3.600
Entradas negativas	Acesse entradas de cache que resultaram na negação de acesso aos clientes.	Mínimo: 60 Máximo: 86.400 Padrão: 3.600

Exemplo

Um cliente NFS tenta acessar um volume em um cluster. O ONTAP corresponde o cliente a uma regra de política de exportação e determina que o cliente obtém acesso com base na configuração da regra de política de exportação. O ONTAP armazena a regra de política de exportação no cache de acesso como uma entrada positiva. Por padrão, o ONTAP mantém a entrada positiva no cache de acesso por uma hora (3.600 segundos) e, em seguida, atualiza automaticamente a entrada para manter as informações atualizadas.

Para evitar que o cache de acesso seja preenchido desnecessariamente, há um parâmetro adicional para limpar entradas de cache de acesso existentes que não foram usadas por um determinado período de tempo para decidir o acesso do cliente. `-harvest-timeout`Este parâmetro tem um intervalo permitido de 60 a 2.592.000 segundos e uma predefinição de 86.400 segundos.

Remova uma política de exportação de uma qtree

Se você decidir que não deseja que uma política de exportação específica seja atribuída

a uma qtree por mais tempo, poderá remover a política de exportação modificando a qtree para herdar a política de exportação do volume que contém. Você pode fazer isso usando o `volume qtree modify` comando com o `-export-policy` parâmetro e uma string de nome vazia ("").

Passos

1. Para remover uma política de exportação de uma qtree, digite o seguinte comando:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Verifique se a qtree foi modificada em conformidade:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Valide as IDs de qtree para operações de arquivos de qtree

O ONTAP pode executar uma validação adicional opcional de IDs de qtree. Essa validação garante que as solicitações de operação de arquivo cliente usem um ID de qtree válido e que os clientes só possam mover arquivos dentro da mesma qtree. Pode ativar ou desativar esta validação modificando o `-validate-qtree-export` parâmetro. Este parâmetro está ativado por predefinição.

Sobre esta tarefa

Esse parâmetro só é efetivo quando você atribuiu uma política de exportação diretamente a um ou mais qtrees na máquina virtual de armazenamento (SVM).

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se pretender que a validação da ID de qtree seja…	Digite o seguinte comando…
Ativado	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Desativado	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Restrições de política de exportação e junções aninhadas para volumes FlexVol

Se você configurou políticas de exportação para definir uma política menos restritiva em uma junção aninhada, mas uma política mais restritiva em uma junção de nível mais alto, o acesso à junção de nível inferior pode falhar.

Você deve garantir que as junções de nível mais alto tenham políticas de exportação menos restritivas do que as junções de nível mais baixo.

Usando Kerberos com NFS para segurança forte

Suporte ONTAP para Kerberos

O Kerberos fornece autenticação segura forte para aplicativos cliente/servidor. A autenticação fornece a verificação de identidades de usuário e processo para um servidor. No ambiente ONTAP, o Kerberos fornece autenticação entre máquinas virtuais de armazenamento (SVMs) e clientes NFS.

No ONTAP 9, a seguinte funcionalidade Kerberos é suportada:

- Autenticação Kerberos 5 com verificação de integridade (krb5i)

  O Krb5i usa checksums para verificar a integridade de cada mensagem NFS transferida entre cliente e servidor. Isso é útil tanto por motivos de segurança (por exemplo, para garantir que os dados não foram adulterados) quanto por motivos de integridade de dados (por exemplo, para evitar a corrupção de dados ao usar NFS em redes não confiáveis).

- Autenticação Kerberos 5 com verificação de privacidade (krb5p)

  Krb5p usa checksums para criptografar todo o tráfego entre o cliente e o servidor. Isto é mais seguro e também incorre mais carga.

- Criptografia AES de 128 bits e 256 bits

  O Advanced Encryption Standard (AES) é um algoritmo de encriptação para proteger dados eletrónicos. O ONTAP suporta AES com chaves de 128 bits (AES-128) e AES com criptografia de chaves de 256 bits (AES-256) para Kerberos para maior segurança.

- Configurações de realm Kerberos no nível da SVM

  Os administradores do SVM agora podem criar configurações do Kerberos Realm no nível SVM. Isso significa que os administradores do SVM não precisam mais confiar no administrador do cluster para a configuração do Kerberos Realm e podem criar configurações individuais do Kerberos Realm em um ambiente de alocação a vários clientes.

Requisitos para configurar Kerberos com NFS

Antes de configurar o Kerberos com NFS no sistema, você deve verificar se determinados itens no ambiente de rede e armazenamento estão configurados corretamente.

As etapas para configurar seu ambiente dependem de qual versão e tipo de sistema operacional cliente, controlador de domínio, Kerberos, DNS, etc. que você está usando. Documentar todas essas variáveis está além do escopo deste documento. Para obter mais informações, consulte a respetiva documentação para cada componente.

Para um exemplo detalhado de como configurar o ONTAP e o Kerberos 5 com NFSv3 e NFSv4 em um ambiente usando o ative Directory do Windows Server 2008 R2 e hosts Linux, consulte o relatório técnico 4073.

Os seguintes itens devem ser configurados primeiro:

Requisitos de ambiente de rede

- Kerberos

  Você deve ter uma configuração Kerberos funcionando com um centro de distribuição de chaves (KDC), como Kerberos baseados no ative Directory do Windows ou MIT Kerberos.

  Os servidores NFS devem usar `nfs` como o componente principal de sua máquina principal.

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como ative Directory ou OpenLDAP, que esteja configurado para usar LDAP em SSL/TLS.

- NTP

  Você deve ter um servidor de tempo de trabalho executando NTP. Isso é necessário para evitar a falha de autenticação Kerberos devido ao desvio de tempo.

- Resolução de nome de domínio (DNS)

  Cada cliente UNIX e cada SVM LIF devem ter um Registro de serviço (SRV) adequado registrado no KDC em zonas de pesquisa direta e inversa. Todos os participantes devem ser solucionáveis corretamente via DNS.

- Contas de utilizador

  Cada cliente deve ter uma conta de usuário no Reino Kerberos. Os servidores NFS devem usar "nfs" como o componente principal de sua máquina principal.

Requisitos do cliente NFS

- NFS

  Cada cliente deve ser configurado corretamente para se comunicar através da rede usando NFSv3 ou NFSv4.

  Os clientes devem suportar RFC1964 e RFC2203.

- Kerberos

  Cada cliente deve ser configurado corretamente para usar a autenticação Kerberos, incluindo os seguintes detalhes:

- A encriptação para comunicação TGS está ativada.

  AES-256 para maior segurança.

- O tipo de encriptação mais seguro para comunicação TGT está ativado.
- O domínio e o domínio Kerberos estão configurados corretamente.
- O GSS está ativado.

  Ao usar credenciais de máquina:

- Não execute `gssd` com o `-n` parâmetro.
- Não execute `kinit` como usuário raiz.

- Cada cliente deve usar a versão mais recente e atualizada do sistema operacional.

  Isso fornece a melhor compatibilidade e confiabilidade para criptografia AES com Kerberos.

- DNS

  Cada cliente deve ser configurado corretamente para usar o DNS para a resolução correta do nome.

- NTP

  Cada cliente deve estar sincronizando com o servidor NTP.

- Informações de host e domínio

  Cada cliente `/etc/hosts` e `/etc/resolv.conf` arquivos devem conter o nome de host correto e as informações de DNS, respetivamente.

- Ficheiros keytab

  Cada cliente deve ter um arquivo keytab do KDC. O Reino deve estar em letras maiúsculas. O tipo de criptografia deve ser AES-256 para maior segurança.

- Opcional: Para obter o melhor desempenho, os clientes se beneficiam de ter pelo menos duas interfaces de rede: Uma para comunicação com a rede local e outra para comunicação com a rede de armazenamento.

Requisitos do sistema de storage

- Licença NFS

  O sistema de storage deve ter uma licença NFS válida instalada.

- Licença CIFS

  A licença CIFS é opcional. Só é necessário para verificar credenciais do Windows ao usar mapeamento de nomes multiprotocolo. Não é necessário em um ambiente restrito somente para UNIX.

- SVM

  Você precisa ter pelo menos um SVM configurado no sistema.

- DNS na SVM

  Você deve ter DNS configurado em cada SVM.

- Servidor NFS

  Você precisa ter o NFS configurado na SVM.

- Criptografia AES

  Para uma segurança mais forte, você deve configurar o servidor NFS para permitir apenas criptografia AES-256 para Kerberos.

- Servidor SMB

  Se você estiver executando um ambiente multiprotocolo, deverá ter o SMB configurado na SVM. O servidor SMB é necessário para o mapeamento de nomes multiprotocolo.

- Volumes

  Você precisa ter um volume raiz e pelo menos um volume de dados configurados para uso pelo SVM.

- Volume raiz

  O volume raiz do SVM precisa ter a seguinte configuração:

Nome	Definição
Estilo de segurança	UNIX
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	777

  Em contraste com o volume raiz, os volumes de dados podem ter um estilo de segurança.

- Grupos UNIX

  O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0
pcuser	65534 (criado automaticamente pelo ONTAP ao criar o SVM)

- Utilizadores UNIX

  O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS O primeiro componente do usuário cliente NFS SPN é usado como usuário.
pcuser	65534	65534	Necessário para uso multiprotocolo NFS e CIFS Criado e adicionado ao grupo pcuser automaticamente pelo ONTAP ao criar o SVM.
raiz	0	0	Necessário para a montagem

  O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.

- Políticas e regras de exportação

  Você deve ter configurado políticas de exportação com as regras de exportação necessárias para os volumes raiz e de dados e qtrees. Se todos os volumes da SVM forem acessados por Kerberos, você poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5` , `krb5i` ou `krb5p`.

- Mapeamento de nomes Kerberos-UNIX

  Se você quiser que o usuário identificado pelo usuário cliente NFS SPN tenha permissões de raiz, você deve criar um mapeamento de nome para root.

Informações relacionadas

"Relatório técnico da NetApp 4073: Autenticação unificada segura"

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Administração do sistema"

"Gerenciamento de storage lógico"

Especifique o domínio de ID de usuário para NFSv4

Para especificar o domínio de ID de usuário, você pode definir a `-v4-id-domain` opção.

Sobre esta tarefa

Por padrão, o ONTAP usa o domínio NIS para o mapeamento de ID de usuário NFSv4, se um estiver definido. Se um domínio NIS não estiver definido, o domínio DNS será usado. Talvez seja necessário definir o domínio de ID de usuário se, por exemplo, você tiver vários domínios de ID de usuário. O nome de domínio deve corresponder à configuração de domínio no controlador de domínio. Não é necessário para NFSv3.

Passo

1. Introduza o seguinte comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Uso do TLS com NFS para uma segurança forte

Visão geral do uso do TLS com NFS para uma segurança forte

O TLS permite comunicações de rede criptografadas com segurança equivalente e menos complexidade do que o Kerberos e o IPsec. Como administrador, você pode habilitar, configurar e desabilitar o TLS para segurança forte com conexões NFSv3 e NFSv4.x usando o Gerenciador de sistema, a CLI do ONTAP ou a API REST do ONTAP.

> O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

O ONTAP usa o TLS 1,3 para conexões NFS em TLS.

Requisitos

O NFS em TLS requer certificados X,509. Você pode criar e instalar um certificado de servidor assinado pela CA no cluster do ONTAP ou instalar um certificado que o serviço NFS usa diretamente. Seus certificados devem atender às seguintes diretrizes:

- O nome comum (CN) de cada certificado deve ser configurado com o nome de domínio totalmente qualificado (FQDN) do LIF de dados no qual o TLS será ativado.
- O nome alternativo do assunto (SAN) de cada certificado deve ser configurado com o endereço IP do LIF de dados no qual o TLS será ativado. Opcionalmente, você pode configurar a SAN com o endereço IP e o FQDN do LIF de dados. Se o endereço IP e o FQDN estiverem configurados, os clientes NFS podem se conetar usando o endereço IP ou o FQDN.
- Você pode instalar vários certificados de serviço NFS para o mesmo LIF, mas apenas um deles pode ser usado de cada vez como parte da configuração TLS NFS.

Ativar ou desativar TLS para clientes NFS no ONTAP

Você pode melhorar a segurança das conexões NFS configurando o NFS em TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS. Você pode configurar isso em uma VM de

storage existente habilitada para NFS.

> O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

- Consulte "requisitos"o para NFS sobre TLS antes de começar.
- Consulte as páginas do manual do ONTAP para obter mais informações sobre o comando neste procedimento.
- Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-nfs-tls-interface-enable.html[`vserver nfs tls interface show` em referência de comando ONTAP.

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) na qual ativar o TLS.
2. Habilite o TLS para conexões NFS nessa VM e interface de storage.

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir habilita o NFS sobre TLS no `data1` LIF da `vs1` VM de storage:

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

Antes de começar

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-nfs-tls-interface-disable.html[`vserver nfs tls interface disable` em referência de comando ONTAP.

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) para desativar o TLS.
2. Desative TLS para conexões NFS nessa VM e interface de storage.

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir desativa NFS sobre TLS no `data1` LIF da `vs1` VM de armazenamento:

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Editar uma configuração TLS

Você pode alterar as configurações de uma configuração NFS em TLS existente. Por exemplo, você pode usar este procedimento para atualizar o certificado TLS.

Antes de começar

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-nfs-tls-interface-modify.html[`vserver nfs tls interface modify` em referência de comando ONTAP.

Passos

1. Escolha uma VM de storage e uma interface lógica (LIF) para modificar a configuração TLS para clientes NFS.
2. Modificar a configuração. Se especificar um `status` de `enable`, também terá de especificar o `certificate-name` parâmetro. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir modifica a configuração NFS sobre TLS no `data2` LIF da `vs2` VM de armazenamento:

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```

Informações relacionadas

"Ative o storage nas para servidores Linux usando NFS".

Configurar serviços de nomes

Como funciona a configuração do switch do serviço de nomes ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

Tipo de banco de dados	Define fontes de serviço de nome para…	Fontes válidas são…
hosts	Conversão de nomes de host para endereços IP	ficheiros, dns
grupo	Procurar informações do grupo de utilizadores	arquivos, nis, ldap
passwd	Procurar informações do utilizador	arquivos, nis, ldap
grupo de rede	Procurar informações do netgroup	arquivos, nis, ldap
namemap	Mapeando nomes de usuários	ficheiros, ldap

Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

Especificar tipo de origem…	Para procurar informações em…	Gerenciado pelas famílias de comando…

ficheiros	Arquivos de origem local	`vserver services name-service unix-user vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	`vserver services name-service ldap`
dns	Servidores DNS externos conforme especificado na configuração DNS do SVM	`vserver services name-service dns`

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

Fonte do serviço de nomes externo	Protocolo utilizado para acesso
NIS	UDP
DNS	UDP
LDAP	TCP

Exemplo

O exemplo a seguir exibe a configuração do switch do serviço de nomes para o SVM_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para procurar endereços IP para hosts, o ONTAP primeiro consulta os arquivos de origem locais. Se a consulta não retornar nenhum resultado, os servidores DNS serão verificados em seguida.

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM.svm_1. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Utilize LDAP

Visão geral do LDAP

Um servidor LDAP (Lightweight Directory Access Protocol) permite manter centralmente as informações do usuário. Se você armazenar seu banco de dados de usuários em um servidor LDAP em seu ambiente, poderá configurar seu sistema de storage para procurar informações de usuário em seu banco de dados LDAP existente.

- Antes de configurar o LDAP para ONTAP, você deve verificar se a implantação do site atende às práticas recomendadas para configuração do servidor LDAP e do cliente. Em especial, devem ser satisfeitas as seguintes condições:
  - O nome de domínio do servidor LDAP deve corresponder à entrada no cliente LDAP.
  - Os tipos de hash de senha do usuário LDAP suportados pelo servidor LDAP devem incluir aqueles suportados pelo ONTAP:
    - CRYPT (todos os tipos) e SHA-1 (SHA, SSHA).
    - A partir do ONTAP 9.8, hashes SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 e SSHA-512) também são suportados.
  - Se o servidor LDAP exigir medidas de segurança de sessão, você deve configurá-las no cliente LDAP.

    As seguintes opções de segurança de sessão estão disponíveis:

        - Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
        - INICIE O TLS
        - LDAPS (LDAP sobre TLS ou SSL)
    - Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
        - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
        - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
        - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
    - Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
        - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
        - Se o LDAPS for usado, o servidor LDAP deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
        - Um servidor de certificados já deve estar configurado no domínio.
    - Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
        - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
            - Bidirecional
            - One-way, onde o primário confia no domínio de referência
            - Pai-filho
        - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
        - As senhas de domínio devem ser iguais para autenticar quando `--bind-as-cifs-server` definidas como verdadeiro.

        As configurações a seguir não são suportadas com a busca por referência LDAP.

        - Para todas as versões do ONTAP:
        - Clientes LDAP em um SVM admin
        - Para o ONTAP 9.8 e versões anteriores (eles são suportados em 9.9.1 e posteriores):
        - Assinatura e selagem LDAP (a `-session-security` opção)
        - Conexões TLS criptografadas (a `-use-start-tls` opção)
        - Comunicações através da porta LDAPS 636 (a `-use-ldaps-for-ad-ldap` opção)

- Começando com ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch."
- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

  Na maioria dos casos, um dos esquemas ONTAP padrão será apropriado. No entanto, se o esquema LDAP em seu ambiente for diferente desses, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar o cliente LDAP. Consulte o administrador LDAP sobre os requisitos para o seu ambiente.

- O uso do LDAP para resolução de nome de host não é suportado.

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você deve configurar as configurações de segurança do servidor NFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`. teste

A assinatura LDAP e a vedação no tráfego SMB são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Conceitos LDAPS

Você deve entender certos termos e conceitos sobre como o ONTAP protege a comunicação LDAP. O ONTAP pode usar TLS ou LDAPS para configurar sessões autenticadas entre servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX.

Terminologia

Existem certos termos que você deve entender sobre como o ONTAP usa o LDAPS para proteger a comunicação LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Um protocolo para acessar e gerenciar diretórios de informações. O LDAP é usado como um diretório de informações para armazenar objetos como usuários, grupos e grupos de rede. O LDAP também fornece serviços de diretório que gerenciam esses objetos e atendem solicitações LDAP de clientes LDAP.

- **SSL**

  (Secure Sockets Layer) Um protocolo desenvolvido para enviar informações de forma segura pela Internet. O SSL é suportado pelo ONTAP 9 e posterior, mas foi obsoleto em favor do TLS.

- **TLS**

  (Transport Layer Security) um protocolo de rastreamento de padrões IETF que é baseado nas especificações SSL anteriores. É o sucessor do SSL. O TLS é compatível com o ONTAP 9.5 e posterior.

- **LDAPS (LDAP sobre SSL ou TLS)**

  Um protocolo que usa TLS ou SSL para proteger a comunicação entre clientes LDAP e servidores LDAP. Os termos *LDAP sobre SSL* e *LDAP sobre TLS* às vezes são usados de forma intercambiável. O LDAPS é suportado pelo ONTAP 9.5 e posterior.

- No ONTAP 9.5-9,8, o LDAPS só pode ser ativado na porta 636. Para fazer isso, use o `-use-ldaps-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.
- A partir do ONTAP 9.9,1, o LDAPS pode ser ativado em qualquer porta, embora a porta 636 permaneça a predefinição. Para fazer isso, defina o `-ldaps-enabled` parâmetro `true` e especifique o parâmetro desejado `-port`. Para obter mais informações, consulte a `vserver services name-service ldap client create` página de manual

É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.

- * Iniciar TLS*

  (Também conhecido como *start_tls*, *STARTTLS* e *STARTTLS*) Um mecanismo para fornecer comunicação segura usando os protocolos TLS.

  O ONTAP usa o STARTTLS para proteger a comunicação LDAP e usa a porta LDAP padrão (389) para se comunicar com o servidor LDAP. O servidor LDAP deve ser configurado para permitir conexões pela porta LDAP 389; caso contrário, as conexões LDAP TLS do SVM ao servidor LDAP falharão.

Como o ONTAP usa o LDAPS

O ONTAP oferece suporte à autenticação de servidor TLS, o que permite que o cliente LDAP SVM confirme a identidade do servidor LDAP durante a operação de vinculação. Os clientes LDAP habilitados para TLS podem usar técnicas padrão de criptografia de chave pública para verificar se o certificado e a ID pública de um servidor são válidos e foram emitidos por uma autoridade de certificação (CA) listada na lista de CAs confiáveis do cliente.

O LDAP suporta STARTTLS para criptografar comunicações usando TLS. O STARTTLS começa como uma conexão de texto simples sobre a porta LDAP padrão (389), e essa conexão é então atualizada para TLS.

O ONTAP oferece suporte ao seguinte:

- LDAPS para tráfego relacionado a SMB entre os servidores LDAP integrados ao ative Directory e o SVM
- LDAPS para tráfego LDAP para mapeamento de nomes e outras informações do UNIX

  Servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX podem ser usados para armazenar informações para mapeamento de nomes LDAP e outras informações do UNIX, como usuários, grupos e netgroups.

- Certificados CA raiz autoassinados

  Ao usar um LDAP integrado do ative-Directory, o certificado raiz autoassinado é gerado quando o Serviço de certificados do Windows Server é instalado no domínio. Ao usar um servidor LDAP baseado em UNIX para mapeamento de nomes LDAP, o certificado raiz autoassinado é gerado e salvo usando meios apropriados para esse aplicativo LDAP.

Por predefinição, o LDAPS está desativado.

Ative o suporte ao LDAP RFC2307bis

Se você quiser usar o LDAP e exigir a capacidade adicional de usar associações a grupos aninhados, você pode configurar o ONTAP para habilitar o suporte ao LDAP RFC2307bis.

O que você vai precisar

Você deve ter criado uma cópia de um dos esquemas de cliente LDAP padrão que você deseja usar.

Sobre esta tarefa

Em esquemas de cliente LDAP, os objetos de grupo usam o atributo memberUid. Esse atributo pode conter vários valores e lista os nomes dos usuários que pertencem a esse grupo. Em esquemas de cliente LDAP habilitados para RFC2307bis, os objetos de grupo usam o atributo uniqueMember. Este atributo pode conter o nome distinto completo (DN) de outro objeto no diretório LDAP. Isso permite que você use grupos aninhados porque os grupos podem ter outros grupos como membros.

O usuário não deve ser membro de mais de 256 grupos, incluindo grupos aninhados. O ONTAP ignora quaisquer grupos acima do limite de 256 grupos.

Por padrão, o suporte a RFC2307bis está desativado.

> O suporte a RFC2307bis é ativado automaticamente no ONTAP quando um cliente LDAP é criado com o esquema MS-AD-BIS.

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Modifique o esquema de cliente LDAP RFC2307 copiado para ativar o suporte RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifique o esquema para corresponder à classe de objeto suportada no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifique o esquema para corresponder ao nome de atributo suportado no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Opções de configuração para pesquisas de diretório LDAP

Você pode otimizar as pesquisas de diretório LDAP, incluindo informações de usuário, grupo e netgroup, configurando o cliente LDAP do ONTAP para se conetar a servidores LDAP da maneira mais apropriada para o seu ambiente. Você precisa entender quando os valores padrão de pesquisa base LDAP e escopo são suficientes e quais parâmetros

especificar quando os valores personalizados são mais apropriados.

As opções de pesquisa de cliente LDAP para informações de usuário, grupo e netgroup podem ajudar a evitar consultas LDAP com falha e, portanto, falha no acesso de cliente aos sistemas de armazenamento. Eles também ajudam a garantir que as pesquisas sejam o mais eficientes possível para evitar problemas de desempenho do cliente.

Valores de pesquisa padrão base e escopo

A base LDAP é o DN base padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o DN base. Essa opção é apropriada quando o diretório LDAP é relativamente pequeno e todas as entradas relevantes estão localizadas no mesmo DN.

Se você não especificar um DN base personalizado, o padrão será `root`. Isso significa que cada consulta pesquisa o diretório inteiro. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

O escopo base LDAP é o escopo de pesquisa padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o escopo base. Ele determina se a consulta LDAP pesquisa somente a entrada nomeada, as entradas um nível abaixo do DN ou toda a subárvore abaixo do DN.

Se você não especificar um escopo base personalizado, o padrão será `subtree`. Isso significa que cada consulta pesquisa a subárvore inteira abaixo do DN. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

Valores de pesquisa de base e escopo personalizados

Opcionalmente, você pode especificar valores de base e escopo separados para pesquisas de usuário, grupo e netgroup. Limitar a base de pesquisa e o escopo das consultas dessa forma pode melhorar significativamente o desempenho, pois limita a pesquisa a uma subseção menor do diretório LDAP.

Se você especificar valores de base e escopo personalizados, eles substituirão a base de pesquisa padrão geral e o escopo para pesquisas de usuário, grupo e netgroup. Os parâmetros para especificar valores de base e escopo personalizados estão disponíveis no nível de privilégio avançado.

Parâmetro cliente LDAP…	Especifica personalizado…
`-base-dn`	DN base para todas as pesquisas LDAP os valores múltiplos podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada no ONTAP 9.5 e versões posteriores).
`-base-scope`	Escopo base para todas as pesquisas LDAP
`-user-dn`	DNS base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário.
`-user-scope`	Escopo base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário.

`-group-dn`	DNS base para todas as pesquisas de grupo LDAP
`-group-scope`	Escopo base para todas as pesquisas de grupo LDAP
`-netgroup-dn`	DNS base para todas as pesquisas de netgroup LDAP
`-netgroup-scope`	Escopo base para todas as pesquisas de netgroup LDAP

Vários valores DN base personalizados

Se a estrutura de diretórios LDAP for mais complexa, poderá ser necessário especificar vários DNS base para procurar determinadas informações em várias partes do diretório LDAP. Você pode especificar vários DNS para os parâmetros DN de usuário, grupo e netgroup separando-os com um ponto e vírgula (;) e anexando toda a lista de pesquisa DN com aspas duplas ("). Se um DN contiver um ponto-e-vírgula, você deve adicionar um caractere de escape imediatamente antes do ponto-e-vírgula no DN.

Observe que o escopo se aplica a toda a lista de DNS especificada para o parâmetro correspondente. Por exemplo, se você especificar uma lista de três DNS de usuário e subárvore diferentes para o escopo do usuário, o usuário LDAP pesquisará toda a subárvore para cada um dos três DNS especificados.

A partir do ONTAP 9.5, você também pode especificar LDAP *referral chasing*, o que permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP não for retornada pelo servidor LDAP primário. O cliente usa esses dados de referência para recuperar o objeto de destino do servidor descrito nos dados de referência. Para procurar objetos presentes nos servidores LDAP referidos, o base-DN dos objetos referidos pode ser adicionado ao base-DN como parte da configuração do cliente LDAP. No entanto, os objetos referidos só são procurados quando a busca por referência está ativada (usando a `-referral-enabled true` opção) durante a criação ou modificação do cliente LDAP.

Melhore o desempenho das pesquisas de diretório LDAP netgroup-by-host

Se o seu ambiente LDAP estiver configurado para permitir pesquisas netgroup-by-host, você poderá configurar o ONTAP para aproveitar isso e realizar pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas do netgroup e reduzir possíveis problemas de acesso ao cliente NFS devido à latência durante as pesquisas do netgroup.

O que você vai precisar

Seu diretório LDAP deve conter um `netgroup.byhost` mapa.

Seus servidores DNS devem conter Registros de pesquisa direta (A) e reversa (PTR) para clientes NFS.

Quando você especifica endereços IPv6 em netgroups, você deve sempre encurtar e compactar cada endereço conforme especificado no RFC 5952.

Sobre esta tarefa

Os servidores NIS armazenam informações do netgroup em três mapas separados chamados `netgroup` `netgroup.byuser` , e `netgroup.byhost`. O objetivo dos `netgroup.byuser` mapas e `netgroup.byhost` é acelerar as pesquisas de netgroup. O ONTAP pode realizar pesquisas netgroup-by-host

em servidores NIS para melhorar os tempos de resposta de montagem.

Por padrão, os diretórios LDAP não têm um `netgroup.byhost` mapa como os servidores NIS. No entanto, é possível, com a ajuda de ferramentas de terceiros, importar um mapa NIS `netgroup.byhost` para diretórios LDAP para permitir pesquisas rápidas netgroup-by-host. Se você tiver configurado seu ambiente LDAP para permitir pesquisas netgroup-by-host, poderá configurar o cliente LDAP do ONTAP com o `netgroup.byhost` nome do mapa, DN e o escopo de pesquisa para pesquisas mais rápidas netgroup-by-host.

Receber os resultados das pesquisas netgroup-by-host com mais rapidez permite que o ONTAP processe regras de exportação com mais rapidez quando os clientes NFS solicitam acesso às exportações. Isso reduz a chance de atraso no acesso devido a problemas de latência de pesquisa do netgroup.

Passos

1. Obtenha o nome distinto completo exato do mapa NIS `netgroup.byhost` importado para o diretório LDAP.

   O DN do mapa pode variar dependendo da ferramenta de terceiros usada para importação. Para obter o melhor desempenho, você deve especificar o DN exato do mapa.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Ative as pesquisas netgroup-by-host na configuração de cliente LDAP da máquina virtual de armazenamento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false`Ativar ou desativar a pesquisa netgroup-by-host para diretórios LDAP. A predefinição é `false`.

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` Especifica o nome distinto do `netgroup.byhost` mapa no diretório LDAP. Ele substitui o DN base para pesquisas netgroup-by-host. Se você não especificar esse parâmetro, o ONTAP usará o DN base.

   `-netgroup-byhost-scope {base|onelevel subtree`especifica o escopo de pesquisa para pesquisas netgroup-by-host. Se não especificar este parâmetro, a predefinição é `subtree`.

   Se a configuração do cliente LDAP ainda não existir, você pode habilitar pesquisas netgroup-by-host especificando esses parâmetros ao criar uma nova configuração de cliente LDAP usando o `vserver services name-service ldap client create` comando.

   > ⓘ A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O comando a seguir modifica a configuração de cliente LDAP existente chamada "ldap_corp" para habilitar pesquisas netgroup-by-host usando o mapa chamado netgroup `netgroup.byhost`.byhost", dc `subtree`

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Depois de terminar

Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente.

Informações relacionadas

"IETF RFC 5952: Uma recomendação para representação de texto de endereço IPv6"

Use LDAP fast bind para autenticação nsswitch

A partir do ONTAP 9.11,1, você pode aproveitar a funcionalidade LDAP *fast bind* (também conhecida como *concurrent bind*) para solicitações de autenticação de cliente mais rápidas e simples. Para utilizar esta funcionalidade, o servidor LDAP tem de suportar a funcionalidade de ligação rápida.

Sobre esta tarefa

Sem vinculação rápida, o ONTAP usa o LDAP Simple BIND para autenticar usuários administrativos com o servidor LDAP. Com esse método de autenticação, o ONTAP envia um nome de usuário ou grupo para o servidor LDAP, recebe a senha de hash armazenada e compara o código de hash do servidor com o código de hash gerado localmente a partir da senha do usuário. Se forem idênticos, o ONTAP concede permissão de login.

Com a funcionalidade de vinculação rápida, o ONTAP envia apenas credenciais de usuário (nome de usuário e senha) para o servidor LDAP por meio de uma conexão segura. Em seguida, o servidor LDAP valida essas credenciais e instrui o ONTAP a conceder permissões de login.

Uma vantagem do fast bind é que não há necessidade de o ONTAP suportar cada novo algoritmo de hash suportado por servidores LDAP, porque o hash de senha é executado pelo servidor LDAP.

"Saiba mais sobre como usar o fast bind."

Você pode usar configurações de cliente LDAP existentes para o LDAP fast bind. No entanto, é altamente recomendável que o cliente LDAP seja configurado para TLS ou LDAPS; caso contrário, a senha é enviada por fio em texto simples.

Para ativar o LDAP fast bind em um ambiente ONTAP, você precisa atender a estes requisitos:

- Os usuários de administração do ONTAP devem ser configurados em um servidor LDAP que suporte a vinculação rápida.
- O SVM do ONTAP deve ser configurado para LDAP no banco de dados de switch de serviços de nome (nsswitch).
- As contas de usuário e grupo de administrador do ONTAP devem ser configuradas para autenticação nsswitch usando vinculação rápida.

Passos

1. Confirme com o administrador LDAP que o LDAP FAST BIND é suportado no servidor LDAP.

2. Certifique-se de que as credenciais de utilizador admin do ONTAP estão configuradas no servidor LDAP.
3. Verifique se o administrador ou SVM de dados está configurado corretamente para o LDAP fast bind.

   a. Para confirmar se o servidor LDAP FAST BIND está listado na configuração do cliente LDAP, introduza:

      `vserver services name-service ldap client show`

      "Saiba mais sobre a configuração do cliente LDAP."

   b. Para confirmar `ldap` que é uma das fontes configuradas para o banco de dados nsswitch `passwd`, digite:

      `vserver services name-service ns-switch show`

   "Saiba mais sobre a configuração do nsswitch."

4. Certifique-se de que os usuários de administração estejam autenticando com o nsswitch e que a autenticação LDAP de vinculação rápida esteja habilitada em suas contas.

   ◦ Para usuários existentes, insira `security login modify` e verifique as seguintes configurações de parâmetro:

      `-authentication-method nsswitch`

`-is-ldap-fastbind true`

   ◦ Para novos utilizadores de administração, consulte "Ative o acesso a contas LDAP ou NIS."

Apresentar estatísticas LDAP

A partir do ONTAP 9.2, você pode exibir estatísticas LDAP para máquinas virtuais de armazenamento (SVMs) em um sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

O que você vai precisar

- Você deve ter configurado um cliente LDAP no SVM.
- Você deve ter objetos LDAP identificados a partir dos quais você pode exibir dados.

Passo

1. Veja os dados de desempenho para objetos de contador:

   `statistics show`

Exemplos

O exemplo a seguir exibe estatísticas para a amostra chamada **smpl_1** para contadores: avg_processor_busy e CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Configurar mapeamentos de nomes

Configure a visão geral dos mapeamentos de nomes

O ONTAP usa mapeamento de nomes para mapear identidades SMB para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades SMB. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conetando a partir de um cliente NFS ou de um cliente SMB.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso SMB ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

  Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo, você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um usuário UNIX específico e para o UID do usuário.

Como o mapeamento de nomes funciona

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um

mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

  Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

  Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário SMB padrão não estiver configurado e o ONTAP não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

  Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do ative Directory com o domínio home do servidor SMB podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor SMB no SVM.

- *Confiança bidirecional*

  Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor SMB tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

  Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

  Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

- *Confiança inbound*

  Com uma confiança de entrada, o outro domínio confia no domínio home do servidor SMB. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

  Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	o administrador do servidor não está habilitado a usar a barra de ferramentas	O usuário UNIX "'root'" é mapeado para o usuário chamado "'administrador'". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.
*	clique no botão "ok"	Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado.  O asterisco é válido apenas para o mapeamento de nomes de UNIX para Windows, e não para o contrário.

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de carateres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie um mapeamento de nomes

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula `" "` (o caractere de espaço). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure o usuário padrão

Você pode configurar um usuário padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Configure o usuário UNIX padrão	`vserver cifs options modify -default-unix-user user_name`
Configure o usuário padrão do Windows	`vserver nfs modify -default-win-user user_name`

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`
Troque a posição de dois mapeamentos de nomes NOTA: Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`
Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consulte a página de manual de cada comando para obter mais informações.

Ative o acesso para clientes Windows NFS

O ONTAP suporta acesso a arquivos de clientes Windows NFSv3. Isso significa que os clientes que executam sistemas operacionais Windows com suporte a NFSv3 podem

acessar arquivos em exportações NFSv3 no cluster. Para usar essa funcionalidade com êxito, você deve configurar corretamente a máquina virtual de storage (SVM) e estar ciente de certos requisitos e limitações.

Sobre esta tarefa

Por padrão, o suporte ao cliente do Windows NFSv3 está desativado.

Antes de começar

O NFSv3 precisa estar habilitado no SVM.

Passos

1. Ativar o suporte ao cliente do Windows NFSv3:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly
   disabled
   ```

2. Em todos os SVMs que suportam clientes Windows NFSv3, desative os `-enable-ejukebox` parâmetros e `-v3-connection-drop`:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection
   -drop disabled
   ```

   Os clientes do Windows NFSv3 agora podem montar exportações no sistema de armazenamento.

3. Certifique-se de que cada cliente do Windows NFSv3 utiliza suportes rígidos especificando a `-o mtype=hard` opção.

   Isso é necessário para garantir montagens confiáveis.

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

Ative a exibição de exportações NFS em clientes NFS

Os clientes NFS podem usar o `showmount -e` comando para ver uma lista de exportações disponíveis a partir de um servidor ONTAP NFS. Isso pode ajudar os usuários a identificar o sistema de arquivos que eles querem montar.

A partir do ONTAP 9.2, o ONTAP permite que os clientes NFS visualizem a lista de exportação por padrão. Em versões anteriores, a `showmount` opção `vserver nfs modify` do comando deve ser ativada explicitamente. Para visualizar a lista de exportação, o NFSv3 deve estar habilitado no SVM.

Exemplo

O comando a seguir mostra o recurso showmount no SVM chamado VS1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

O comando a seguir executado em um cliente NFS exibe a lista de exportações em um servidor NFS com o endereço IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Gerenciar o acesso a arquivos usando NFS

Ativar ou desativar NFSv3

Pode ativar ou desativar o NFSv3 modificando a `-v3` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv3. Por padrão, NFSv3 está ativado.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Desativar NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Ativar ou desativar NFSv4,0

Pode ativar ou desativar o NFSv4,0 modificando a `-v4.0` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv4,0. No ONTAP 9.9,1, o NFSv4,0 é ativado por padrão; em versões anteriores, ele é desativado por padrão.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	**Digite o seguinte comando…**
Ativar NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Desativar NFSv4,0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Ativar ou desativar NFSv4,1

Pode ativar ou desativar o NFSv4,1 modificando a `-v4.1` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv4,1. No ONTAP 9.9,1, o NFSv4,1 é ativado por padrão; em versões anteriores, ele é desativado por padrão.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ativar NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Desativar NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Gerenciar NFSv4 limites de storepool

A partir do ONTAP 9.13, os administradores podem habilitar seus servidores NFSv4 para negar recursos a clientes NFSv4 quando eles tiverem atingido os limites de recursos do storepool de clientes. Quando os clientes consomem muitos recursos do storepool de NFSv4 isso pode levar a outros clientes NFSv4 serem bloqueados devido à indisponibilidade de recursos do storepool de NFSv4.

Ativar esse recurso também permite que os clientes visualizem o consumo de recursos do storepool ativo por cada cliente. Isso facilita a identificação de clientes que esgotam os recursos do sistema e possibilita impor limites de recursos por cliente.

Veja os recursos do storepool consumidos

O `vserver nfs storepool show` comando mostra o número de recursos do storepool consumidos. Um storepool é um pool de recursos usado por clientes NFSv4.

Passo

1. Como administrador, execute o `vserver nfs storepool show` comando para exibir as informações do storepool de clientes NFSv4.

Exemplo

Este exemplo exibe as informações do storepool de clientes NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Ative ou desative os controles de limite do storepool

Os administradores podem usar os seguintes comandos para ativar ou desativar os controles de limite do storepool.

Passo

1. Como administrador, execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ative os controles de limite do storepool	`vserver nfs storepool config modify -limit-enforce enabled`
Desative os controles de limite do storepool	`vserver nfs storepool config modify -limit-enforce disabled`

Exibir uma lista de clientes bloqueados

Se o limite storepool estiver ativado, os administradores poderão ver quais clientes foram bloqueados ao atingir o limite de recursos por cliente. Os administradores podem usar o seguinte comando para ver quais clientes foram marcados como clientes bloqueados.

Passos

1. Use o `vserver nfs storepool blocked-client show` comando para exibir a lista de clientes bloqueados do NFSv4.

Remova um cliente da lista de clientes bloqueados

Os clientes que atingirem seu limite por cliente serão desconetados e adicionados ao cache block-client. Os administradores podem usar o seguinte comando para remover o cliente do cache de cliente de bloco. Isso permitirá que o cliente se conete ao servidor ONTAP NFSv4.

Passos

1. Use o `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando para lavar o cache de cliente bloqueado storepool.
2. Use o `vserver nfs storepool blocked-client show` comando para verificar se o cliente foi removido do cache de cliente de bloco.

Exemplo

Este exemplo exibe um cliente bloqueado com o endereço IP "10,2.1,1" sendo lavado de todos os nós.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Ative ou desative o pNFS

O pNFS melhora o desempenho permitindo que os clientes NFS executem operações de leitura/gravação em dispositivos de storage diretamente e em paralelo, ignorando o servidor NFS como um potencial gargalo. Para ativar ou desativar pNFS (NFS paralelo), pode modificar a `-v4.1-pnfs` opção.

Se a versão ONTAP for…	O padrão pNFS é…
9,8 ou posterior	desativado
9,7 ou anterior	ativado

O que você vai precisar

O suporte NFSv4,1 é necessário para poder usar o pNFS.

Se você quiser ativar o pNFS, primeiro você deve desativar as referências NFS. Ambos não podem ser ativados ao mesmo tempo.

Se você usar pNFS com Kerberos em SVMs, você deverá habilitar o Kerberos em cada LIF na SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Desativar pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Informações relacionadas

- Visão geral do trunking NFS

Controle o acesso NFS por TCP e UDP

Você pode ativar ou desativar o acesso NFS a máquinas virtuais de armazenamento (SVMs) em TCP e UDP, modificando os `-tcp` parâmetros e `-udp`, respetivamente. Isso permite que você controle se os clientes NFS podem acessar dados via TCP ou UDP em seu ambiente.

Sobre esta tarefa

Estes parâmetros aplicam-se apenas ao NFS. Não afetam protocolos auxiliares. Por exemplo, se o NFS sobre TCP estiver desativado, as operações de montagem sobre TCP ainda terão êxito. Para bloquear completamente o tráfego TCP ou UDP, você pode usar regras de política de exportação.

> Você deve desativar o SnapDiff RPC Server antes de desativar o TCP para NFS para evitar um erro de falha de comando. Você pode desativar o TCP usando o comando `vserver snapdiff-rpc-server off -vserver vserver name`.

Passo

1. Execute uma das seguintes ações:

Se você quiser que o acesso NFS seja…	Digite o comando…
Ativado em TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Desativado por TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Ativado em UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Desativado por UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Controle solicitações NFS de portas não reservadas

Você pode rejeitar solicitações de montagem NFS de portas não reservadas habilitando

a `-mount-rootonly` opção. Para rejeitar todas as solicitações NFS de portas não reservadas, você pode ativar a `-nfs-rootonly` opção.

Sobre esta tarefa

Por padrão, a opção `-mount-rootonly` é `enabled`.

Por padrão, a opção `-nfs-rootonly` é `disabled`.

Estas opções não se aplicam ao procedimento NULL.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Permitir solicitações de montagem NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rejeitar solicitações de montagem NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Permitir todas as solicitações NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Rejeitar todas as solicitações NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Lidar com o acesso NFS a volumes NTFS ou qtrees para usuários UNIX desconhecidos

Se o ONTAP não conseguir identificar usuários UNIX tentando se conetar a volumes ou qtrees com estilo de segurança NTFS, ele não poderá mapear explicitamente o usuário para um usuário do Windows. Você pode configurar o ONTAP para negar acesso a esses usuários para segurança mais rigorosa ou mapeá-los para um usuário padrão do Windows para garantir um nível mínimo de acesso para todos os usuários.

O que você vai precisar

Um usuário padrão do Windows deve ser configurado se você quiser habilitar essa opção.

Sobre esta tarefa

Se um usuário UNIX tentar acessar volumes ou qtrees com estilo de segurança NTFS, o usuário UNIX deve primeiro ser mapeado para um usuário do Windows para que o ONTAP possa avaliar adequadamente as permissões NTFS. No entanto, se o ONTAP não conseguir procurar o nome do usuário UNIX nas fontes de serviço de nome de informações de usuário configuradas, ele não poderá mapear explicitamente o usuário UNIX para um usuário específico do Windows. Você pode decidir como lidar com esses usuários UNIX desconhecidos das seguintes maneiras:

- Negar acesso a usuários UNIX desconhecidos.

  Isso impõe segurança mais rigorosa, exigindo mapeamento explícito para todos os usuários UNIX para

obter acesso a volumes NTFS ou qtrees.

- Mapeie usuários UNIX desconhecidos para um usuário padrão do Windows.

  Isso fornece menos segurança, mas mais conveniência, garantindo que todos os usuários obtenham um nível mínimo de acesso a volumes NTFS ou qtrees por meio de um usuário padrão do Windows.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser o usuário padrão do Windows para usuários UNIX desconhecidos…	Digite o comando…
Ativado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Desativado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Considerações para clientes que montam exportações NFS usando uma porta não reservada

A `-mount-rootonly` opção deve ser desativada em um sistema de armazenamento que deve suportar clientes que montam exportações NFS usando uma porta não reservada mesmo quando o usuário está conetado como raiz. Tais clientes incluem clientes Hummingbird e clientes Solaris NFS/IPv6.

Se a `-mount-rootonly` opção estiver ativada, o ONTAP não permitirá que clientes NFS que usam portas não reservadas, ou seja, portas com números superiores a 1.023, montem exportações NFS.

Execute uma verificação de acesso mais rigorosa para netgroups verificando domínios

Por padrão, o ONTAP executa uma verificação adicional ao avaliar o acesso do cliente para um netgroup. A verificação adicional garante que o domínio do cliente corresponda à configuração do domínio da máquina virtual de armazenamento (SVM). Caso contrário, o ONTAP nega acesso ao cliente.

Sobre esta tarefa

Quando o ONTAP avalia regras de política de exportação para acesso de cliente e uma regra de política de exportação contém um netgroup, o ONTAP deve determinar se o endereço IP de um cliente pertence ao netgroup. Para isso, o ONTAP converte o endereço IP do cliente para um nome de host usando DNS e obtém um nome de domínio totalmente qualificado (FQDN).

Se o arquivo netgroup apenas listar um nome curto para o host e o nome curto para o host existir em vários domínios, é possível que um cliente de um domínio diferente obtenha acesso sem essa verificação.

Para evitar isso, o ONTAP compara o domínio retornado do DNS para o host com a lista de nomes de domínio DNS configurados para o SVM. Se corresponder, o acesso é permitido. Se não corresponder, o acesso é negado.

Esta verificação está ativada por predefinição. Você pode gerenciá-lo modificando o `-netgroup-dns -domain-search` parâmetro, que está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você deseja que a verificação de domínio para netgroups seja…	Digite…
Ativado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Desativado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Defina o nível de privilégio como admin:

   ```
   set -privilege admin
   ```

Modifique as portas usadas para serviços NFSv3

O servidor NFS no sistema de armazenamento usa serviços como o daemon de montagem e o Gerenciador de bloqueio de rede para se comunicar com clientes NFS através de portas de rede padrão específicas. Na maioria dos ambientes NFS, as portas padrão funcionam corretamente e não exigem modificação, mas se você quiser usar diferentes portas de rede NFS em seu ambiente NFSv3, você pode fazer isso.

O que você vai precisar

A alteração das portas NFS no sistema de storage exige que todos os clientes NFS se reconetem ao sistema. Portanto, você deve comunicar essas informações aos usuários antes de fazer a alteração.

Sobre esta tarefa

Você pode definir as portas usadas pelos serviços de daemon de montagem NFS, Network Lock Manager, Network Status Monitor e NFS quota daemon para cada máquina virtual de armazenamento (SVM). A alteração do número da porta afeta os clientes NFS que acessam dados por TCP e UDP.

As portas para NFSv4 e NFSv4,1 não podem ser alteradas.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Desativar o acesso ao NFS:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Defina a porta NFS para o serviço NFS específico:

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

Parâmetro da porta NFS	Descrição	Porta predefinida
`-mountd-port`	Daemon de montagem NFS	635
`-nlm-port`	Gerenciador de bloqueio de rede	4045
`-nsm-port`	Monitor de estado da rede	4046
`-rquotad-port`	Daemon de cota NFS	4049

   Além da porta padrão, o intervalo permitido de números de porta é de 1024 a 65535. Cada serviço NFS precisa usar uma porta única.

4. Ativar acesso ao NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Use o `network connections listening show` comando para verificar as alterações no número da porta.
6. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

Os comandos a seguir definem a porta NFS Mount Daemon como 1113 no SVM chamado VS1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Comandos para gerenciar servidores NFS

Existem comandos ONTAP específicos para gerenciar servidores NFS.

Se você quiser…	Use este comando…
Crie um servidor NFS	`vserver nfs create`
Exibir servidores NFS	`vserver nfs show`
Modificar um servidor NFS	`vserver nfs modify`
Excluir um servidor NFS	`vserver nfs delete`

Oculte a `.snapshot` lista de diretórios em NFSv3 pontos de montagem O acesso explícito ao `.snapshot` diretório ainda será permitido mesmo que a opção esteja ativada.	`vserver nfs` comandos com a `-v3-hide-snapshot` opção ativada

Consulte a página de manual de cada comando para obter mais informações.

Solucionar problemas do serviço de nomes

Quando os clientes experimentam falhas de acesso devido a problemas de serviço de nome, você pode usar a `vserver services name-service getxxbyyy` família de comandos para executar manualmente várias pesquisas de serviço de nome e examinar os detalhes e resultados da pesquisa para ajudar na solução de problemas.

Sobre esta tarefa

- Para cada comando, você pode especificar o seguinte:
  - Nome do nó ou da máquina virtual de storage (SVM) para realizar a pesquisa.

    Isso permite testar pesquisas de serviços de nomes para um nó específico ou SVM para restringir a pesquisa de um possível problema de configuração de serviço de nomes.
  - Se deve mostrar a fonte usada para a pesquisa.

    Isso permite verificar se a fonte correta foi usada.
- O ONTAP seleciona o serviço para realizar a pesquisa com base na ordem configurada do switch do serviço de nomes.
- Esses comandos estão disponíveis no nível avançado de privilégio.

Passos

1. Execute uma das seguintes ações:

Para recuperar…	Use o comando…
Endereço IP de um nome de host	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Apenas endereços IPv4)
Membros de um grupo por ID de grupo	`vserver services name-service getxxbyyy getgrbygid`

Membros de um grupo por nome de grupo	`vserver services name-service getxxbyyy getgrbyname`
Lista de grupos aos quais um usuário pertence	`vserver services name-service getxxbyyy getgrlist`
Nome do host de um endereço IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Apenas endereços IPv4)
Informações do usuário por nome de usuário	`vserver services name-service getxxbyyy getpwbyname` É possível testar a resolução de nomes de usuários do RBAC especificando o `-use-rbac` parâmetro como `true`.
Informações do usuário por ID do usuário	`vserver services name-service getxxbyyy getpwbyuid` É possível testar a resolução de nomes de usuários do RBAC especificando o `-use-rbac` parâmetro como `true`.
A associação netgroup de um cliente	`vserver services name-service getxxbyyy netgrp`
A associação netgroup de um cliente usando a pesquisa netgroup-by-host	`vserver services name-service getxxbyyy netgrpbyhost`

O exemplo a seguir mostra um teste de pesquisa de DNS para o SVM VS1 ao tentar obter o endereço IP do host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

O exemplo a seguir mostra um teste de pesquisa NIS para o SVM VS1 ao tentar recuperar informações de usuário para um usuário com o UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

O exemplo a seguir mostra um teste de pesquisa LDAP para o SVM VS1 ao tentar recuperar informações de usuário para um usuário com o nome ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

O exemplo a seguir mostra um teste de pesquisa de netgroup para o SVM VS1 ao tentar descobrir se o cliente dnshost0 é membro do netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analise os resultados do teste realizado e tome a ação necessária.

Se o…	Veja o…
A pesquisa de nome de host ou endereço IP falhou ou gerou resultados incorretos	Configuração DNS
A pesquisa consultou uma fonte incorreta	Configuração do switch do serviço de nomes

Se o…	Veja o…
A pesquisa de usuário ou grupo falhou ou produziu resultados incorretos	• Configuração do switch do serviço de nomes • Configuração de origem (arquivos locais, domínio NIS, cliente LDAP) • Configuração de rede (por exemplo, LIFs e rotas)
A pesquisa de nomes de host falhou ou expirou, e o servidor DNS não resolve nomes curtos de DNS (por exemplo, host1)	Configuração de DNS para consultas de domínio de topo (TLD). Você pode desabilitar consultas TLD usando a `-is-tld-query-enabled false` opção para o `vserver services name-service dns modify` comando.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Verifique as conexões do serviço de nomes

A partir do ONTAP 9.2, pode verificar os servidores de nomes DNS e LDAP para verificar se estão ligados ao ONTAP. Esses comandos estão disponíveis no nível de privilégios de administrador.

Sobre esta tarefa

Você pode verificar se há uma configuração válida do serviço de nomes DNS ou LDAP conforme necessário usando o verificador de configuração do serviço de nomes. Esta verificação de validação pode ser iniciada na linha de comando ou no System Manager.

Para configurações de DNS, todos os servidores são testados e precisam estar funcionando para que a configuração seja considerada válida. Para configurações LDAP, desde que qualquer servidor esteja ativo, a configuração é válida. Os comandos do serviço de nomes aplicam o verificador de configuração a menos que o `skip-config-validation` campo seja verdadeiro (o padrão é falso).

Passo

1. Use o comando apropriado para verificar uma configuração do serviço de nomes. A IU exibe o status dos servidores configurados.

Para verificar…	Use este comando…
Estado da configuração DNS	`vserver services name-service dns check`
Estado da configuração LDAP	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

A validação da configuração é bem-sucedida se pelo menos um dos servidores configurados (name-serviders/ldap-serviders) estiver acessível e fornecendo o serviço. É apresentado um aviso se alguns dos servidores não estiverem acessíveis.

Comandos para gerenciar entradas do switch do serviço de nomes

Você pode gerenciar entradas de switch de serviço de nomes criando, exibindo, modificando e excluindo-as.

Se você quiser…	Use este comando…
Crie uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch create`
Exibir entradas do switch de serviço de nomes	`vserver services name-service ns-switch show`
Modificar uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch modify`
Excluir uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch delete`

Consulte a página de manual de cada comando para obter mais informações.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Comandos para gerenciar o cache do serviço de nomes

Você pode gerenciar o cache do serviço de nomes modificando o valor time to live (TTL). O valor TTL determina quanto tempo as informações do serviço de nome são persistentes no cache.

Se você quiser modificar o valor TTL para…	Use este comando…
Usuários UNIX	`vserver services name-service cache unix-user settings`
Grupos UNIX	`vserver services name-service cache unix-group settings`
Netgroups UNIX	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Associação ao grupo	`vserver services name-service cache group-membership settings`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`
Troque a posição de dois mapeamentos de nomes NOTA: Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`

Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar usuários UNIX locais

Existem comandos ONTAP específicos para gerenciar usuários UNIX locais.

Se você quiser…	Use este comando…
Crie um usuário local do UNIX	`vserver services name-service unix-user create`
Carregue usuários UNIX locais a partir de um URI	`vserver services name-service unix-user load-from-uri`
Exibir usuários locais do UNIX	`vserver services name-service unix-user show`
Modifique um usuário local UNIX	`vserver services name-service unix-user modify`
Excluir um usuário local UNIX	`vserver services name-service unix-user delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar grupos UNIX locais

Existem comandos ONTAP específicos para gerenciar grupos UNIX locais.

Se você quiser…	Use este comando…
Crie um grupo UNIX local	`vserver services name-service unix-group create`
Adicione um usuário a um grupo UNIX local	`vserver services name-service unix-group adduser`
Carregue grupos UNIX locais a partir de um URI	`vserver services name-service unix-group load-from-uri`
Exibir grupos UNIX locais	`vserver services name-service unix-group show`
Modifique um grupo UNIX local	`vserver services name-service unix-group modify`

Excluir um usuário de um grupo UNIX local	`vserver services name-service unix-group deluser`
Exclua um grupo UNIX local	`vserver services name-service unix-group delete`

Consulte a página de manual de cada comando para obter mais informações.

Limites para usuários, grupos e membros do grupo UNIX locais

O ONTAP introduziu limites para o número máximo de usuários e grupos UNIX no cluster e comandos para gerenciar esses limites. Esses limites podem ajudar a evitar problemas de desempenho, impedindo que os administradores criem muitos usuários e grupos UNIX locais no cluster.

Há um limite para o número combinado de grupos de usuários UNIX locais e membros de grupo. Há um limite separado para usuários UNIX locais. Os limites são em todo o cluster. Cada um desses novos limites é definido como um valor padrão que você pode modificar até um limite rígido pré-atribuído.

Banco de dados	Limite padrão	Limite rígido
Usuários locais do UNIX	32.768	65.536
Grupos UNIX locais e membros do grupo	32.768	65.536

Gerenciar limites para usuários e grupos UNIX locais

Existem comandos ONTAP específicos para gerenciar limites para usuários e grupos UNIX locais. Os administradores de cluster podem usar esses comandos para solucionar problemas de desempenho no cluster que se acredita estar relacionado a um número excessivo de usuários e grupos UNIX locais.

Sobre esta tarefa

Esses comandos estão disponíveis para o administrador do cluster no nível avançado de privilégio.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Use o comando…
Exibir informações sobre os limites de usuários UNIX locais	`vserver services unix-user max-limit show`
Exibir informações sobre os limites de grupos UNIX locais	`vserver services unix-group max-limit show`

Se você quiser…	Use o comando…
Modifique os limites de usuários UNIX locais	`vserver services unix-user max-limit modify`
Modificar limites de grupo UNIX local	`vserver services unix-group max-limit modify`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar netgroups locais

É possível gerenciar grupos de redes locais carregando-os a partir de um URI, verificando seu status entre nós, exibindo-os e excluindo-os.

Se você quiser…	Use o comando…
Carregue netgroups de um URI	`vserver services name-service netgroup load`
Verifique o status dos grupos de redes entre nós	`vserver services name-service netgroup status` Disponível no nível de privilégio avançado e superior.
Exibir grupos de redes locais	`vserver services name-service netgroup file show`
Exclua um netgroup local	`vserver services name-service netgroup file delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações de domínio NIS

Existem comandos ONTAP específicos para gerenciar configurações de domínio NIS.

Se você quiser…	Use este comando…
Crie uma configuração de domínio NIS	`vserver services name-service nis-domain create`
Exibir configurações de domínio NIS	`vserver services name-service nis-domain show`
Exibir status de vinculação de uma configuração de domínio NIS	`vserver services name-service nis-domain show-bound`
Apresentar estatísticas NIS	`vserver services name-service nis-domain show-statistics` Disponível no nível de privilégio avançado e superior.

Limpar estatísticas NIS	`vserver services name-service nis-domain clear-statistics` Disponível no nível de privilégio avançado e superior.
Modificar uma configuração de domínio NIS	`vserver services name-service nis-domain modify`
Excluir uma configuração de domínio NIS	`vserver services name-service nis-domain delete`
Ative o armazenamento em cache para pesquisas netgroup-by-host	`vserver services name-service nis-domain netgroup-database config modify` Disponível no nível de privilégio avançado e superior.

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações de cliente LDAP

Existem comandos ONTAP específicos para gerenciar configurações de cliente LDAP.

> Os administradores do SVM não podem modificar ou excluir configurações de cliente LDAP criadas pelos administradores de cluster.

Se você quiser…	Use este comando…
Crie uma configuração de cliente LDAP	`vserver services name-service ldap client create`
Exibir configurações de cliente LDAP	`vserver services name-service ldap client show`
Modificar uma configuração de cliente LDAP	`vserver services name-service ldap client modify`
Altere a senha DE VINCULAÇÃO do cliente LDAP	`vserver services name-service ldap client modify-bind-password`
Eliminar uma configuração de cliente LDAP	`vserver services name-service ldap client delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações LDAP

Existem comandos ONTAP específicos para gerenciar configurações LDAP.

Se você quiser…	Use este comando…
Crie uma configuração LDAP	`vserver services name-service ldap create`

Exibir configurações LDAP	`vserver services name-service ldap show`
Modificar uma configuração LDAP	`vserver services name-service ldap modify`
Eliminar uma configuração LDAP	`vserver services name-service ldap delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar modelos de esquema de cliente LDAP

Existem comandos ONTAP específicos para gerenciar modelos de esquema de cliente LDAP.

Os administradores do SVM não podem modificar ou excluir esquemas de cliente LDAP criados por administradores de cluster.

Se você quiser…	Use este comando…
Copie um modelo de esquema LDAP existente	`vserver services name-service ldap client schema copy` Disponível no nível de privilégio avançado e superior.
Exibir modelos de esquema LDAP	`vserver services name-service ldap client schema show`
Modifique um modelo de esquema LDAP	`vserver services name-service ldap client schema modify` Disponível no nível de privilégio avançado e superior.
Excluir um modelo de esquema LDAP	`vserver services name-service ldap client schema delete` Disponível no nível de privilégio avançado e superior.

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações de interface NFS Kerberos

Existem comandos ONTAP específicos para gerenciar configurações de interface do NFS Kerberos.

Se você quiser…	Use este comando…
Ative o NFS Kerberos em um LIF	`vserver nfs kerberos interface enable`
Exibir configurações de interface NFS Kerberos	`vserver nfs kerberos interface show`
Modificar uma configuração de interface NFS Kerberos	`vserver nfs kerberos interface modify`

Desative o NFS Kerberos em um LIF	`vserver nfs kerberos interface disable`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações NFS Kerberos Realm

Existem comandos ONTAP específicos para gerenciar configurações de realm Kerberos NFS.

Se você quiser…	Use este comando…
Crie uma configuração NFS Kerberos realm	`vserver nfs kerberos realm create`
Exibir configurações do NFS Kerberos Realm	`vserver nfs kerberos realm show`
Modifique uma configuração de realm do Kerberos NFS	`vserver nfs kerberos realm modify`
Excluir uma configuração NFS Kerberos realm	`vserver nfs kerberos realm delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar políticas de exportação

Existem comandos ONTAP específicos para gerenciar políticas de exportação.

Se você quiser…	Use este comando…
Exibir informações sobre políticas de exportação	`vserver export-policy show`
Renomeie uma política de exportação	`vserver export-policy rename`
Copiar uma política de exportação	`vserver export-policy copy`
Eliminar uma política de exportação	`vserver export-policy delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar regras de exportação

Existem comandos ONTAP específicos para gerenciar regras de exportação.

Se você quiser…	Use este comando…
Crie uma regra de exportação	`vserver export-policy rule create`
Exibir informações sobre regras de exportação	`vserver export-policy rule show`
Modificar uma regra de exportação	`vserver export-policy rule modify`
Excluir uma regra de exportação	`vserver export-policy rule delete`

Se você tiver configurado várias regras de exportação idênticas que correspondam a diferentes clientes, certifique-se de mantê-las sincronizadas ao gerenciar regras de exportação.

Consulte a página de manual de cada comando para obter mais informações.

Configurar o cache de credenciais NFS

Motivos para modificar o tempo de funcionamento do cache de credenciais NFS

O ONTAP usa um cache de credenciais para armazenar as informações necessárias para autenticação de usuário para acesso de exportação NFS para fornecer acesso mais rápido e melhorar o desempenho. Você pode configurar por quanto tempo as informações são armazenadas no cache de credenciais para personalizá-las para o seu ambiente.

Há vários cenários ao modificar o cache de credenciais NFS Time-to-live (TTL) pode ajudar a resolver problemas. Você deve entender quais são esses cenários, bem como as consequências de fazer essas modificações.

Razões

Considere alterar o TTL padrão nas seguintes circunstâncias:

Problema	Medidas corretivas
Os servidores de nomes no seu ambiente estão sofrendo degradação no desempenho devido a uma alta carga de solicitações do ONTAP.	Aumente o TTL para credenciais positivas e negativas armazenadas em cache para reduzir o número de solicitações do ONTAP para servidores de nomes.
O administrador do servidor de nomes fez alterações para permitir o acesso a usuários NFS que foram negados anteriormente.	Diminua o TTL para credenciais negativas armazenadas em cache para reduzir o tempo que os usuários NFS precisam esperar que o ONTAP solicite novas credenciais de servidores de nomes externos para que eles possam obter acesso.

Problema	Medidas corretivas
O administrador do servidor de nomes fez alterações para negar acesso a usuários NFS que anteriormente eram permitidos.	Reduza o TTL para credenciais positivas armazenadas em cache para reduzir o tempo antes que o ONTAP solicite novas credenciais de servidores de nomes externos para que os usuários NFS agora tenham acesso negado.

Consequências

Você pode modificar o tempo individualmente para armazenar credenciais positivas e negativas em cache. No entanto, você deve estar ciente das vantagens e desvantagens de fazê-lo.

Se você…	A vantagem é…	A desvantagem é…
Aumente o tempo de cache de credenciais positivas	O ONTAP envia solicitações de credenciais para nomear servidores com menos frequência, reduzindo a carga nos servidores de nomes.	Leva mais tempo para negar acesso a usuários NFS que anteriormente eram permitidos acesso, mas não são mais.
Diminua o tempo de cache positivo de credenciais	Leva menos tempo para negar acesso a usuários NFS que anteriormente eram permitidos acesso, mas não são mais.	O ONTAP envia solicitações de credenciais para nomear servidores com mais frequência, aumentando a carga nos servidores de nomes.
Aumente o tempo de cache de credenciais negativas	O ONTAP envia solicitações de credenciais para nomear servidores com menos frequência, reduzindo a carga nos servidores de nomes.	Leva mais tempo para conceder acesso a usuários NFS que anteriormente não tinham acesso permitido, mas agora.
Diminua o tempo de cache de credenciais negativas	Leva menos tempo para conceder acesso a usuários NFS que anteriormente não tinham acesso permitido, mas agora.	O ONTAP envia solicitações de credenciais para nomear servidores com mais frequência, aumentando a carga nos servidores de nomes.

Configure o tempo de ativação para credenciais de usuário NFS armazenadas em cache

Você pode configurar o período de tempo que o ONTAP armazena credenciais para usuários NFS em seu cache interno (time-to-live ou TTL) modificando o servidor NFS da máquina virtual de armazenamento (SVM). Isso permite que você solucione certos problemas relacionados à alta carga nos servidores de nomes ou alterações nas credenciais que afetam o acesso do usuário NFS.

Sobre esta tarefa

Estes parâmetros estão disponíveis no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você quiser modificar o TTL para cache…	Use o comando…
Credenciais positivas	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` O TTL é medido em milissegundos. A partir do ONTAP 9.10,1 e posterior, o padrão é de 1 hora (3.600.000 milissegundos). No ONTAP 9.9,1 e anterior, o padrão é 24 horas (86.400.000 milissegundos). O intervalo permitido para este valor é de 1 minuto (60000 milissegundos) a 7 dias (604.800.000 milissegundos).
Credenciais negativas	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` O TTL é medido em milissegundos. O padrão é 2 horas (7.200.000 milissegundos). O intervalo permitido para este valor é de 1 minuto (60000 milissegundos) a 7 dias (604.800.000 milissegundos).

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar caches de política de exportação

Lavar caches de política de exportação

O ONTAP usa vários caches de política de exportação para armazenar informações relacionadas a políticas de exportação para acesso mais rápido. A eliminação de caches de política de exportação manualmente (`vserver export-policy cache flush`) remove informações potencialmente desatualizadas e força o ONTAP a recuperar informações atuais dos recursos externos apropriados. Isso pode ajudar a resolver uma variedade de problemas relacionados ao acesso do cliente às exportações NFS.

Sobre esta tarefa

As informações de cache de política de exportação podem estar desatualizadas devido aos seguintes motivos:

- Uma alteração recente às regras de política de exportação
- Uma alteração recente nos registos de nome de anfitrião nos servidores de nomes
- Uma alteração recente para entradas de netgroup em servidores de nomes
- Recuperando-se de uma interrupção de rede que impedia que os netgroups fossem totalmente

carregados

Passos

1. Se você não tiver o cache do serviço de nomes habilitado, execute uma das seguintes ações no modo de privilégio avançado:

Se você quiser flush…	Digite o comando…
Todos os caches de política de exportação (exceto showmount)	`vserver export-policy cache flush -vserver vserver_name`
As regras de política de exportação acedem à cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Você pode incluir o parâmetro opcional `-node` para especificar o nó no qual deseja limpar o cache de acesso.
O cache do nome do host	`vserver export-policy cache flush -vserver vserver_name -cache host`
O cache netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` O processamento de netgroups é intensivo em recursos. Você só deve limpar o cache do netgroup se estiver tentando resolver um problema de acesso de cliente causado por um netgroup obsoleto.
O cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Se o cache do serviço de nomes estiver ativado, execute uma das seguintes ações:

Se você quiser flush…	Digite o comando…
As regras de política de exportação acedem à cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Você pode incluir o parâmetro opcional `-node` para especificar o nó no qual deseja limpar o cache de acesso.
O cache do nome do host	`vserver services name-service cache hosts forward-lookup delete-all`

Se você quiser flush…	Digite o comando…
O cache netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` O processamento de netgroups é intensivo em recursos. Você só deve limpar o cache do netgroup se estiver tentando resolver um problema de acesso de cliente causado por um netgroup obsoleto.
O cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Exiba a fila e o cache do netgroup da política de exportação

O ONTAP usa a fila netgroup ao importar e resolver netgroups e usa o cache netgroup para armazenar as informações resultantes. Ao solucionar problemas relacionados ao netgroup da política de exportação, você pode usar os `vserver export-policy netgroup queue show` comandos e `vserver export-policy netgroup cache show` para exibir o status da fila do netgroup e o conteúdo do cache do netgroup.

Passo

1. Execute uma das seguintes ações:

Para exibir o netgroup da política de exportação…	Digite o comando…
Fila de espera	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Consulte a página de manual de cada comando para obter mais informações.

Verifique se um endereço IP de cliente é membro de um netgroup

Ao solucionar problemas de acesso de cliente NFS relacionados a netgroups, você pode usar o `vserver export-policy netgroup check-membership` comando para ajudar a determinar se um IP de cliente é membro de um determinado netgroup.

Sobre esta tarefa

Verificar a associação ao netgroup permite determinar se o ONTAP está ciente de que um cliente é ou não membro de um netgroup. Ele também permite que você saiba se o cache do ONTAP netgroup está em um estado transitório enquanto atualiza informações do netgroup. Essas informações podem ajudá-lo a entender por que um cliente pode ter acesso inesperadamente concedido ou negado.

Passo

1. Verifique a associação do netgroup de um endereço IP de cliente: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   O comando pode retornar os seguintes resultados:

   - O cliente é um membro do netgroup.

     Isso foi confirmado por meio de uma pesquisa de pesquisa reversa ou de uma pesquisa netgroup-by-host.

   - O cliente é um membro do netgroup.

     Ele foi encontrado no cache do ONTAP netgroup.

   - O cliente não é membro do netgroup.
   - A associação ao cliente ainda não pode ser determinada porque o ONTAP está atualizando o cache do netgroup.

     Até que isso seja feito, a associação não pode ser explicitamente descartada dentro ou fora. Use o `vserver export-policy netgroup queue show` comando para monitorar o carregamento do netgroup e tentar novamente a verificação depois que ela estiver concluída.

Exemplo

O exemplo a seguir verifica se um cliente com o endereço IP 172.17.16.72 é membro do netgroup Mercury no SVM VS1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Otimizar o desempenho do cache de acesso

Você pode configurar vários parâmetros para otimizar o cache de acesso e encontrar o equilíbrio certo entre o desempenho e a corrente das informações armazenadas no cache de acesso.

Sobre esta tarefa

Quando configurar os períodos de atualização do cache de acesso, tenha em mente o seguinte:

- Valores mais altos significam que as entradas permanecem mais longas no cache de acesso.

  A vantagem é o melhor desempenho porque o ONTAP gasta menos recursos na atualização de entradas de cache de acesso. A desvantagem é que se as regras de política de exportação mudarem e as entradas de cache de acesso ficarem obsoletas como resultado, leva mais tempo para atualizá-las. Como resultado, os clientes que devem obter acesso podem ser negados e os clientes que devem ser negados podem obter acesso.

- Valores mais baixos significam que o ONTAP atualiza as entradas do cache de acesso com mais frequência.

A vantagem é que as entradas são mais atuais e os clientes são mais propensos a ter acesso correto ou negado. A desvantagem é uma diminuição no desempenho porque o ONTAP gasta mais recursos atualizando entradas de cache de acesso.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Para modificar o…	Digite…
Período de atualização para entradas positivas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Período de atualização para entradas negativas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Período de tempo limite para entradas antigas	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Verifique as novas configurações de parâmetros:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm` , `rmdir` e `mv` podem

causar falha no aplicativo NFS.

- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB deny-read e deny-write, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um bytelock SMB exclusivo.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.
- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.

> As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança da Lista de Controle de Acesso (ACL) do Windows que impedem que usuários ou aplicativos renomeem diretórios críticos.

Saiba mais "Como impedir que diretórios sejam renomeados enquanto os clientes os acessam"sobre o .

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4,1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.
- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho . O modo de acesso sharelock é write-deny_none, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de write-deny_none para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
```

```
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Travas de quebra

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

   A página de manual do comando contém informações detalhadas.

2. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

3. Execute uma das seguintes ações:

Se você quiser quebrar um bloqueio especificando…	Digite o comando…
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
A ID de bloqueio	`vserver locks break -lockid UUID`

4. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Como os filtros de primeira leitura e primeira gravação do FPolicy funcionam com o NFS

Os clientes NFS experimentam um alto tempo de resposta durante o alto tráfego de solicitações de leitura/gravação quando o FPolicy é habilitado usando um servidor FPolicy externo com operações de leitura/gravação como eventos monitorados. Para clientes NFS, o uso de filtros de primeira leitura e primeira gravação no FPolicy reduz o número de notificações do FPolicy e melhora o desempenho.

No NFS, o cliente faz a e/S em um arquivo, buscando sua alça. Esse identificador pode permanecer válido nas reinicializações do servidor e do cliente. Portanto, o cliente está livre para armazenar em cache o identificador e enviar solicitações nele sem recuperar alças novamente. Em uma sessão regular, muitas solicitações de leitura/gravação são enviadas para o servidor de arquivos. Se as notificações forem geradas para todas essas solicitações, isso pode resultar nos seguintes problemas:

- Uma carga maior devido ao processamento de notificação adicional e maior tempo de resposta.
- Um grande número de notificações sendo enviadas para o servidor FPolicy, mesmo que o servidor não seja afetado por todas as notificações.

Depois de receber a primeira solicitação de leitura/gravação de um cliente para um arquivo específico, uma entrada de cache é criada e a contagem de leitura/gravação é incrementada. Essa solicitação é marcada como a operação de primeira leitura/gravação e um evento FPolicy é gerado. Antes de Planejar e criar seus filtros FPolicy para um cliente NFS, você deve entender os conceitos básicos de como os filtros FPolicy funcionam.

- Primeira leitura: Filtra as solicitações de leitura do cliente para primeira leitura.

  Quando esse filtro é usado para eventos NFS, as `-file-session-io-grouping-count` configurações e `-file-session-io-grouping-duration` determinam a solicitação de primeira leitura para a qual o FPolicy é processado.

- Primeira gravação: Filtra as solicitações de gravação do cliente para a primeira gravação.

  Quando esse filtro é usado para eventos NFS, as `-file-session-io-grouping-count` configurações e `-file-session-io-grouping-duration` determinam a solicitação de primeira gravação para a qual o FPolicy foi processado.

As seguintes opções são adicionadas no banco de dados de servidores NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modifique a ID de implementação do servidor NFSv4,1

O protocolo NFSv4,1 inclui uma ID de implementação de servidor que documenta o domínio, o nome e a data do servidor. Você pode modificar os valores padrão da ID de implementação do servidor. Alterar os valores padrão pode ser útil, por exemplo, ao coletar estatísticas de uso ou solucionar problemas de interoperabilidade. Para obter mais informações, consulte RFC 5661.

Sobre esta tarefa

Os valores padrão para as três opções são os seguintes:

Opção	Nome da opção	Valor padrão
Domínio ID de implementação NFSv4,1	`-v4.1-implementation -domain`	NetApp.com
NFSv4,1 Nome ID implementação	`-v4.1-implementation-name`	Nome da versão do cluster
NFSv4,1 Data ID implementação	`-v4.1-implementation-date`	Data da versão do cluster

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser modificar o ID de implementação do NFSv4,1…	Digite o comando…
Domínio	`vserver nfs modify -v4.1 -implementation-domain domain`
Nome	`vserver nfs modify -v4.1 -implementation-name name`
Data	`vserver nfs modify -v4.1 -implementation-date date`

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Gerenciar ACLs NFSv4

Benefícios de habilitar ACLs NFSv4

Há muitos benefícios em habilitar ACLs NFSv4.

Os benefícios de habilitar ACLs NFSv4 incluem o seguinte:

- Controle mais refinado do acesso do usuário para arquivos e diretórios
- Melhor segurança NFS
- Interoperabilidade aprimorada com CIFS
- Remoção da limitação NFS de 16 grupos por usuário

Como as ACLs NFSv4 funcionam

Um cliente que usa ACLs NFSv4 pode definir e exibir ACLs em arquivos e diretórios no sistema. Quando um novo arquivo ou subdiretório é criado em um diretório que tem uma ACL, o novo arquivo ou subdiretório herda todas as entradas de controle de acesso (ACEs) na ACL que foram marcadas com os sinalizadores de herança apropriados.

Quando um arquivo ou diretório é criado como resultado de uma solicitação NFSv4, a ACL no arquivo ou diretório resultante depende se a solicitação de criação de arquivo inclui uma ACL ou apenas permissões de acesso de arquivo UNIX padrão e se o diretório pai tem uma ACL:

- Se a solicitação incluir uma ACL, essa ACL é usada.
- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão, mas o diretório pai tiver uma ACL, os ACEs na ACL do diretório pai serão herdados pelo novo arquivo ou diretório, desde que os ACEs tenham sido marcados com os sinalizadores de herança apropriados.

  Uma ACL pai é herdada mesmo se `-v4.0-acl` estiver definida como `off`.

- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão e o diretório pai não tiver uma ACL, o modo de arquivo cliente será usado para definir permissões de acesso a arquivos UNIX padrão.
- Se a solicitação incluir apenas permissões de acesso de arquivo UNIX padrão e o diretório pai tiver uma ACL não herdável, o novo objeto será criado apenas com bits de modo.

Se o `-chown-mode` parâmetro tiver sido definido como `restricted` com comandos nas `vserver nfs` famílias ou `vserver export-policy rule`, a propriedade do arquivo só pode ser alterada pelo superusuário, mesmo que as permissões no disco definidas com ACLs NFSv4 permitam que um usuário não-root altere a propriedade do arquivo. Para obter mais informações, consulte as páginas de manual relevantes.

Ativar ou desativar a modificação das ACLs NFSv4

Quando o ONTAP recebe um `chmod` comando para um arquivo ou diretório com uma ACL, por padrão a ACL é mantida e modificada para refletir a alteração de bit de modo. Você pode desativar o `-v4-acl-preserve` parâmetro para alterar o comportamento se quiser que a ACL seja descartada.

Sobre esta tarefa

Ao usar estilo de segurança unificado, esse parâmetro também especifica se as permissões de arquivo NTFS são preservadas ou descartadas quando um cliente envia um comando chmod, chgroup ou chown para um arquivo ou diretório.

A predefinição para este parâmetro está ativada.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ativar retenção e modificação de ACLs NFSv4 existentes (padrão)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Desative a retenção e solte as ACLs NFSv4 ao alterar os bits de modo	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como o ONTAP usa ACLs NFSv4 para determinar se ele pode excluir um arquivo

Para determinar se ele pode excluir um arquivo, o ONTAP usa uma combinação do bit DE EXCLUSÃO do arquivo e o bit DELETE_CHILD do diretório que contém. Para obter mais informações, consulte o NFS 4,1 RFC 5661.

Ativar ou desativar ACLs NFSv4

Para ativar ou desativar as ACLs NFSv4, pode modificar as `-v4.0-acl` opções e. `-v4.1-acl` Estas opções estão desativadas por predefinição.

Sobre esta tarefa

A `-v4.0-acl` opção ou `-v4.1-acl` controla a configuração e visualização de ACLs NFSv4; ela não controla a aplicação dessas ACLs para verificação de acesso.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar ACLs NFSv4,0	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Desativar ACLs NFSv4,0	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Ativar ACLs NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Desativar ACLs NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modifique o limite máximo de ACE para ACLs NFSv4

É possível modificar o número máximo de ACEs permitidos para cada ACL NFSv4 modificando o parâmetro `-v4-acl-max-aces`. Por padrão, o limite é definido como 400 ACEs para cada ACL. Aumentar esse limite pode ajudar a garantir a migração bem-sucedida de dados com ACLs que contêm mais de 400 ACEs para sistemas de storage que executam ONTAP.

Sobre esta tarefa

Aumentar esse limite pode afetar o desempenho dos clientes que acessam arquivos com ACLs NFSv4.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Modifique o limite máximo de ACE para ACLs NFSv4:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   O intervalo válido de

   `max_ace_limit` é a. `192` `1024`.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Gerenciar delegações de arquivos do NFSv4

Ativar ou desativar as delegações de ficheiros de leitura do NFSv4

Para ativar ou desativar as delegações de ficheiros de leitura do NFSv4, pode modificar a `-v4.0-read-delegation`opção ou . Ao ativar as delegações de arquivos de leitura, você pode eliminar grande parte da sobrecarga de mensagens associada à abertura e fechamento de arquivos.

Sobre esta tarefa

Por padrão, as delegações de arquivos de leitura são desativadas.

A desvantagem de habilitar delegações de arquivos de leitura é que o servidor e seus clientes devem recuperar delegações após o servidor reiniciar ou reiniciar, um cliente reiniciar ou reiniciar, ou uma partição de rede ocorrer.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar as delegações de ficheiros de leitura NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Ativar as delegações de ficheiros de leitura NFSv4,1	Introduza o seguinte comando: E `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Desativar as delegações de ficheiros de leitura NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Desativar as delegações de ficheiros de leitura NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Resultado

As opções de delegação de arquivos entram em vigor assim que são alteradas. Não há necessidade de reinicializar ou reiniciar o NFS.

Ativar ou desativar as delegações de ficheiros de gravação NFSv4

Para ativar ou desativar as delegações de ficheiros de gravação, pode modificar a `-v4.0-write-delegation`opção ou . Ao ativar as delegações de arquivos de gravação, você pode eliminar grande parte da sobrecarga de mensagens associada ao bloqueio de arquivos e Registros, além de abrir e fechar arquivos.

Sobre esta tarefa

Por padrão, as delegações de arquivos de gravação são desativadas.

A desvantagem de habilitar delegações de arquivos de gravação é que o servidor e seus clientes devem executar tarefas adicionais para recuperar delegações após o servidor reiniciar ou reiniciar, um cliente reiniciar ou reiniciar ou uma partição de rede ocorrer.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Ativar as delegações de ficheiros de gravação NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Desativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Desativar as delegações de ficheiros de gravação NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Resultado

As opções de delegação de arquivos entram em vigor assim que são alteradas. Não há necessidade de reinicializar ou reiniciar o NFS.

Configure o bloqueio de arquivos NFSv4 e Registro

Cerca de NFSv4 arquivo e Registro de bloqueio

Para clientes NFSv4, o ONTAP suporta o mecanismo de bloqueio de arquivos NFSv4, mantendo o estado de todos os bloqueios de arquivos em um modelo baseado em leasing.

"Relatório técnico da NetApp 3580: NFSv4 melhorias e melhores práticas Guia de implementação do Data ONTAP"

Especifique o período de locação de bloqueio NFSv4

Para especificar o período de locação de bloqueio NFSv4 (ou seja, o período de tempo em que o ONTAP concede irrevogavelmente um bloqueio a um cliente), você pode modificar a `-v4-lease-seconds` opção. Períodos de leasing mais curtos aceleram a recuperação do servidor, enquanto períodos de leasing mais longos são benéficos para servidores que lidam com uma grande quantidade de clientes.

Sobre esta tarefa

Por padrão, essa opção está definida como `30`. O valor mínimo para esta opção é `10`. O valor máximo para esta opção é o período de tolerância de bloqueio, que pode ser definido com a `locking.lease_seconds` opção.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Especifique o período de tolerância de bloqueio NFSv4

Para especificar o período de carência de bloqueio NFSv4 (ou seja, o período de tempo em que os clientes tentam recuperar seu estado de bloqueio do ONTAP durante a recuperação do servidor), você pode modificar a `-v4-grace-seconds` opção.

Sobre esta tarefa

Por padrão, essa opção está definida como `45`.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como NFSv4 referências funcionam

Quando você ativa referências NFSv4, o ONTAP fornece referências "intra-SVM" para clientes NFSv4. A referência intra-SVM ocorre quando um nó de cluster que recebe a solicitação NFSv4 refere o cliente NFSv4 a outra interface lógica (LIF) na máquina virtual de storage (SVM).

O cliente NFSv4 deve acessar o caminho que recebeu a referência no LIF de destino a partir desse ponto. O nó do cluster original fornece tal referência quando determina que existe um LIF no SVM que reside no nó do cluster no qual o volume de dados reside, permitindo assim aos clientes acesso mais rápido aos dados e evitando comunicação extra do cluster.

Ativar ou desativar referências NFSv4

Você pode habilitar referências NFSv4D em máquinas virtuais de armazenamento (SVMs) habilitando as opções `-v4-fsid-change` e `-v4.0-referrals`ou. Habilitar referências NFSv4 pode resultar em acesso mais rápido aos dados para clientes NFSv4 que suportam esse recurso.

O que você vai precisar

Se você quiser ativar as referências NFS, primeiro desative o NFS paralelo. Não é possível ativar ambos ao mesmo tempo.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar NFSv4 referências	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Desative as referências NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Ativar NFSv4,1 referências	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Desative as referências NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exibir estatísticas NFS

É possível exibir estatísticas NFS para máquinas virtuais de storage (SVMs) no sistema de storage para monitorar a performance e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos NFS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object nfs*
   ```

2. Use os `statistics start` comandos e opcionais `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Exemplo: Monitorando o desempenho do NFSv3

O exemplo a seguir mostra os dados de desempenho do protocolo NFSv3.

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

O comando a seguir mostra os dados da amostra especificando contadores que mostram o número de solicitações de leitura e gravação bem-sucedidas versus o número total de solicitações de leitura e gravação:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Exibir estatísticas de DNS

Você pode exibir estatísticas de DNS para máquinas virtuais de armazenamento (SVMs) no sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos DNS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use os `statistics start` comandos e `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Monitoramento de estatísticas de DNS

Os exemplos a seguir mostram dados de desempenho para consultas DNS. Os seguintes comandos iniciam a coleta de dados para uma nova amostra:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

O comando a seguir exibe dados da amostra especificando contadores que exibem o número de consultas DNS enviadas versus o número de consultas DNS recebidas, com falha ou com tempo limite:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

O comando a seguir exibe dados da amostra especificando contadores que exibem o número de vezes que um erro específico foi recebido para uma consulta DNS no servidor específico:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Apresentar estatísticas NIS

Você pode exibir estatísticas NIS para máquinas virtuais de armazenamento (SVMs) no sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos NIS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use os `statistics start` comandos e `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Monitoramento de estatísticas NIS

Os exemplos a seguir exibem dados de desempenho para consultas NIS. Os seguintes comandos iniciam a coleta de dados para uma nova amostra:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

O comando a seguir exibe dados da amostra especificando contadores que mostram o número de consultas NIS enviadas versus o número de consultas NIS recebidas, com falha ou com tempo limite:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

O comando a seguir exibe dados da amostra especificando contadores que mostram o número de vezes que um erro específico foi recebido para uma consulta NIS no servidor específico:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                            YP_NOTFOUND
    server_ip_address                                     10.227.13.221
3 entries were displayed.
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Suporte para VMware vStorage sobre NFS

O ONTAP dá suporte a determinados recursos de APIs de storage do VMware vStorage para integração de array (VAAI) em um ambiente NFS.

Recursos suportados

Os seguintes recursos são suportados:

- Descarga de cópia

  Permite que um host ESXi copie máquinas virtuais ou discos de máquinas virtuais (VMDKs) diretamente entre o local de armazenamento de dados de origem e destino sem envolver o host. Isso conserva os ciclos de CPU do host ESXi e a largura de banda da rede. A descarga de cópia preserva a eficiência de espaço se o volume de origem for esparso.

- Reserva de espaço

  Garante espaço de armazenamento para um arquivo VMDK reservando espaço para ele.

Limitações

O VMware vStorage sobre NFS tem as seguintes limitações:

- As operações de descarga de cópia podem falhar nos seguintes cenários:
  - Ao executar o wafliron no volume de origem ou destino, porque ele temporariamente coloca o volume off-line
  - Ao mover o volume de origem ou destino
  - Ao mover o LIF de origem ou destino
  - Durante a realização de operações de takeover ou giveback
  - Durante a execução de operações de comutação ou switchback
- A cópia do lado do servidor pode falhar devido a diferenças de formato de identificador de arquivo no seguinte cenário:

  Você tenta copiar dados de SVMs que exportaram qtrees atualmente ou anteriormente para SVMs que nunca exportaram qtrees. Para contornar essa limitação, você pode exportar pelo menos uma qtree no SVM de destino.

Informações relacionadas

"Quais operações descarregadas da VAAI são suportadas pelo Data ONTAP?"

Ative ou desative o VMware vStorage em NFS

Você pode ativar ou desativar o suporte para VMware vStorage sobre NFS em máquinas virtuais de armazenamento (SVMs) usando o `vserver nfs modify` comando.

Sobre esta tarefa

Por padrão, o suporte ao VMware vStorage sobre NFS está desativado.

Passos

1. Exibir o status atual de suporte do vStorage para SVMs:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Habilite o suporte ao VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Desative o suporte ao VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Depois de terminar

Você deve instalar o plug-in NFS para VMware VAAI antes de usar essa funcionalidade. Para obter mais informações, consulte *Instalando o plug-in NFS do NetApp para VMware VAAI*.

Informações relacionadas

"Documentação do NetApp: Plug-in NFS do NetApp para VMware VAAI"

Ativar ou desativar o suporte rquota

O ONTAP suporta o protocolo de cota remota versão 1 (rquota v1). O protocolo rquota permite que os clientes NFS obtenham informações de quota para os utilizadores a partir de uma máquina remota. Você pode ativar o rquota em máquinas virtuais de armazenamento (SVMs) usando o `vserver nfs modify` comando.

Sobre esta tarefa

Por padrão, rquota está desativada.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Habilite o suporte a rquota para SVMs	`vserver nfs modify -vserver vserver_name -rquota enable`
Desative o suporte rquota para SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

   Para obter mais informações sobre cotas, "Gerenciamento de storage lógico"consulte .

Melhoria do desempenho NFSv3 e NFSv4 modificando o tamanho da transferência TCP

Você pode melhorar o desempenho de clientes NFSv3 e NFSv4 conetados a sistemas de armazenamento em uma rede de alta latência, modificando o tamanho máximo de

transferência TCP.

Quando os clientes acessam sistemas de armazenamento em uma rede de alta latência, como uma rede de área ampla (WAN) ou uma rede de área metropolitana (MAN) com latência superior a 10 milissegundos, talvez você consiga melhorar o desempenho da conexão modificando o tamanho máximo da transferência TCP. Os clientes que acessam sistemas de storage em uma rede de baixa latência, como uma rede de área local (LAN), podem esperar pouco ou nenhum benefício ao modificar esses parâmetros. Se a melhoria da taxa de transferência não exceder o impactos da latência, você não deve usar esses parâmetros.

Para determinar se o ambiente de storage se beneficiaria da modificação desses parâmetros, primeiro você deve realizar uma avaliação abrangente de desempenho de um cliente NFS com baixa performance. Analise se o baixo desempenho é devido à latência excessiva da viagem de ida e volta e à pequena solicitação no cliente. Nestas condições, o cliente e o servidor não podem utilizar totalmente a largura de banda disponível porque gastam a maioria dos seus ciclos de serviço esperando que pequenas solicitações e respostas sejam transmitidas através da conexão.

Ao aumentar o tamanho da solicitação NFSv3 e NFSv4, o cliente e o servidor podem usar a largura de banda disponível de forma mais eficaz para mover mais dados por unidade de tempo; portanto, aumentando a eficiência geral da conexão.

Tenha em mente que a configuração entre o sistema de armazenamento e o cliente pode variar. O sistema de armazenamento e o cliente suportam o tamanho máximo de 1 MB para operações de transferência. No entanto, se você configurar o sistema de armazenamento para suportar o tamanho máximo de transferência de 1 MB, mas o cliente só suporta 64 KB, então o tamanho de transferência de montagem é limitado a 64 KB ou menos.

Antes de modificar esses parâmetros, você deve estar ciente de que isso resulta em consumo de memória adicional no sistema de armazenamento pelo período de tempo necessário para montar e transmitir uma grande resposta. Quanto mais conexões de alta latência para o sistema de armazenamento, maior o consumo de memória adicional. Sistemas de armazenamento com alta capacidade de memória podem ter muito pouco efeito com essa mudança. Os sistemas de armazenamento com baixa capacidade de memória podem sofrer uma degradação notável do desempenho.

O uso bem-sucedido desses parâmetros depende da capacidade de recuperar dados de vários nós de um cluster. A latência inerente da rede do cluster pode aumentar a latência geral da resposta. A latência geral tende a aumentar ao usar esses parâmetros. Como resultado, workloads sensíveis à latência podem mostrar impacto negativo.

Modifique o tamanho máximo de transferência do TCP NFSv3 e NFSv4

Você pode modificar a `-tcp-max-xfer-size` opção para configurar tamanhos máximos de transferência para todas as conexões TCP usando os protocolos NFSv3 e NFSv4.x.

Sobre esta tarefa

Você pode modificar essas opções individualmente para cada máquina virtual de storage (SVM).

A partir do ONTAP 9, as `v3-tcp-max-read-size` opções e `v3-tcp-max-write-size` são obsoletas. Você deve usar a `-tcp-max-xfer-size` opção em vez disso.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Modifique o tamanho máximo de transferência do TCP NFSv3 ou NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Opção	Alcance	Padrão
`-tcp-max-xfer-size`	8192 a 1048576 bytes	65536 bytes

> O tamanho máximo de transferência que você inserir deve ser um múltiplo de 4 KB (4096 bytes). As solicitações que não estão alinhadas corretamente afetam negativamente o desempenho.

3. Use o `vserver nfs show -fields tcp-max-xfer-size` comando para verificar as alterações.
4. Se algum cliente usar montagens estáticas, desmonte e remonte para que o novo tamanho de parâmetro entre em vigor.

Exemplo

O comando a seguir define o tamanho máximo de transferência TCP NFSv3 e NFSv4.x para 1048576 bytes no SVM chamado VS1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configure o número de IDs de grupo permitidas para usuários NFS

Por padrão, o ONTAP suporta até 32 IDs de grupo ao lidar com credenciais de usuário NFS usando autenticação Kerberos (RPCSEC_GSS). Ao usar a autenticação AUTH_SYS, o número máximo padrão de IDs de grupo é 16, conforme definido na RFC 5531. Você pode aumentar o máximo até 1.024 se tiver usuários que são membros de mais do que o número padrão de grupos.

Sobre esta tarefa

Se um usuário tiver mais do que o número padrão de IDs de grupo em suas credenciais, os IDs de grupo restantes serão truncados e o usuário poderá receber erros ao tentar acessar arquivos do sistema de armazenamento. Você deve definir o número máximo de grupos, por SVM, para um número que represente o máximo de grupos no ambiente.

> Para entender os pré-requisitos de autenticação AUTH_SYS para ativar grupos estendidos (`-auth-sys-extended-groups`) que usam IDs de grupo além do máximo padrão de 16, consulte este artigo da base de dados de Conhecimento: "AUTH_SYS grupos estendidos alterações para autenticação NFS para ONTAP 9".

A tabela a seguir mostra os dois parâmetros `vserver nfs modify` do comando que determinam o número máximo de IDs de grupo em três configurações de amostra:

Parâmetros	Definições	Limite de IDs de grupo resultantes

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Estas são as predefinições.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se pretender definir o número máximo de grupos auxiliares permitidos…	Digite o comando…
Apenas para RPCSEC_GSS e deixar AUTH_SYS definido para o valor padrão 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Para RPCSEC_GSS e AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verifique o `-extended-groups-limit` valor e verifique se AUTH_SYS está usando grupos estendidos: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

O exemplo a seguir habilita grupos estendidos para autenticação AUTH_SYS e define o número máximo de

grupos estendidos para 512 para autenticação AUTH_SYS e RPCSEC_GSS. Essas alterações são feitas apenas para clientes que acessam o SVM chamado VS1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Controle o acesso do usuário raiz aos dados de estilo de segurança NTFS

Você pode configurar o ONTAP para permitir que clientes NFS acessem dados de estilo de segurança NTFS e clientes NTFS para acessar dados de estilo de segurança NFS. Ao usar o estilo de segurança NTFS em um armazenamento de dados NFS, você deve decidir como tratar o acesso pelo usuário raiz e configurar a máquina virtual de armazenamento (SVM) de acordo.

Sobre esta tarefa

Quando um usuário raiz acessa dados de estilo de segurança NTFS, você tem duas opções:

- Mapeie o usuário raiz para um usuário do Windows como qualquer outro usuário NFS e gerencie o acesso de acordo com ACLs NTFS.
- Ignore as ACLs NTFS e forneça acesso total à raiz.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você quiser que o usuário root…	Digite o comando…
Ser mapeado para um usuário do Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`

Ignorar a verificação da ACL NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

Por predefinição, este parâmetro está desativado.

Se este parâmetro estiver ativado, mas não houver mapeamento de nomes para o usuário raiz, o ONTAP usará uma credencial de administrador SMB padrão para auditoria.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Versões e clientes de NFS compatíveis

Visão geral das versões e clientes NFS compatíveis

Antes de poder usar o NFS na rede, você precisa saber quais versões e clientes do ONTAP são compatíveis.

Esta tabela observa quando versões maiores e menores do protocolo NFS são suportadas por padrão no ONTAP. O suporte por padrão não indica que esta é a versão mais antiga do ONTAP que suporta esse protocolo NFS.

Versão	Suportado	Introduzido
NFSv3	Sim	Todos os lançamentos do ONTAP
NFSv4.0	Sim	ONTAP 8
NFSv4.1	Sim	ONTAP 8,1
NFSv4.2	Sim	ONTAP 9,8
PNFS	Sim	ONTAP 8,1

Para obter as informações mais recentes sobre quais clientes NFS ONTAP suportam, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

NFSv4,0 funcionalidade suportada pelo ONTAP

O ONTAP suporta todas as funcionalidades obrigatórias no NFSv4,0, exceto os mecanismos de segurança SPKM3 e LIPKEY.

A seguinte funcionalidade NFSv4 é suportada:

- **COMPOSTO**

Permite que um cliente solicite várias operações de arquivo em uma única solicitação RPC (chamada de procedimento remoto).

- * Delegação de arquivos*

  Permite que o servidor delege o controle de arquivos a alguns tipos de clientes para acesso de leitura e gravação.

- **Pseudo-fs**

  Usado por servidores NFSv4 para determinar pontos de montagem no sistema de armazenamento. Não existe nenhum protocolo de montagem no NFSv4.

- **Bloqueio**

  Baseado em leasing. Não existem protocolos NLM (Network Lock Manager) ou NSM (Network Status Monitor) separados no NFSv4.

Para obter mais informações sobre o protocolo NFSv4,0, consulte RFC 3530.

Limitações do suporte do ONTAP para NFSv4

Você deve estar ciente de várias limitações do suporte do ONTAP para NFSv4.

- O recurso de delegação não é suportado por todos os tipos de cliente.
- No ONTAP 9.4 e versões anteriores, nomes com carateres não-ASCII em volumes diferentes de UTF8 volumes são rejeitados pelo sistema de armazenamento.

  No ONTAP 9.5 e versões posteriores, os volumes criados com a configuração de linguagem utf8mb4 e montados usando NFS v4 não estão mais sujeitos a essa restrição.

- Todos os identificadores de arquivo são persistentes; o servidor não fornece alças de arquivo voláteis.
- Migração e replicação não são compatíveis.
- Os clientes NFSv4 não são suportados com espelhos de compartilhamento de carga somente leitura.

  O ONTAP encaminha clientes NFSv4 para a fonte do espelho de compartilhamento de carga para acesso direto de leitura e gravação.

- Atributos nomeados não são suportados.
- Todos os atributos recomendados são suportados, exceto para o seguinte:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`

- time_backup

> Embora não ofereça suporte aos `quota*` atributos, o ONTAP oferece suporte a cotas de usuário e grupo por meio do protocolo RQUOTA de banda lateral.

Suporte ONTAP para NFSv4,1

A partir do ONTAP 9.8, a funcionalidade nconnect está disponível por predefinição quando o NFSv4,1 está ativado.

Implementações anteriores de clientes NFS usam apenas uma única conexão TCP com uma montagem. No ONTAP, uma única conexão TCP pode se tornar um gargalo com o aumento de IOPS. No entanto, um cliente habilitado para nconnect pode ter várias conexões TCP (até 16) associadas a uma única montagem NFS. Tal cliente NFS multiplexa operações de arquivos em várias conexões TCP de forma round-robin e, assim, obtém maior throughput da largura de banda de rede disponível. O nConnect é recomendado apenas para montagens NFSv3 e NFSv4,1.

Consulte a documentação do cliente NFS para confirmar se o nconnect é suportado na versão do cliente.

NFSv4,1 é ativado por padrão no ONTAP 9.9,1 e posterior. Em versões anteriores, você pode habilitá-la especificando a `-v4.1` opção e definindo-a para `enabled` quando criar um servidor NFS na máquina virtual de armazenamento (SVM).

O ONTAP não suporta delegações de nível de diretório e arquivo NFSv4,1.

Suporte ONTAP para NFSv4,2

A partir do ONTAP 9.8, o ONTAP suporta o protocolo NFSv4,2 para permitir acesso a clientes habilitados para NFSv4,2.

NFSv4,2 é ativado por padrão no ONTAP 9.9,1 e posterior. No ONTAP 9.8, é necessário habilitar manualmente o v4,2 especificando a `-v4.1` opção e definindo-a para `enabled` quando criar um servidor NFS na máquina virtual de armazenamento (SVM). Ativar o NFSv4,1 também permite que os clientes usem os recursos do NFSv4,1 enquanto montados como v4,2.

Versões sucessivas do ONTAP expandem o suporte para NFSv4,2 recursos opcionais.

Começando com…	NFSv4,2 recursos opcionais incluem …
ONTAP 9.12,1	• Atributos estendidos do NFS • Ficheiros esparsos • Reservas de espaço
ONTAP 9.9,1	Controlo de Acesso obrigatório (MAC) identificado como NFS

Etiquetas de segurança NFS v4,2

A partir do ONTAP 9.9,1, os rótulos de segurança NFS podem ser ativados. Eles são desativados por padrão.

Com os rótulos de segurança NFS v4,2, os servidores ONTAP NFS são cientes do Controle de Acesso

obrigatório (MAC), armazenando e recuperando atributos SEC_label enviados pelos clientes.

Para obter mais informações, "RFC 7240"consulte .

A partir do ONTAP 9.12,1, as etiquetas de segurança NFS v4,2 são compatíveis com operações de despejo NDMP. Se rótulos de segurança forem encontrados em arquivos ou diretórios em versões anteriores, o despejo falhará.

Passos

1. Altere a configuração de privilégios para avançado:

```
set -privilege advanced
```

2. Ativar etiquetas de segurança:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Atributos estendidos do NFS

A partir do ONTAP 9.12,1, os atributos estendidos NFS (xattrs) são ativados por padrão.

Atributos estendidos são atributos NFS padrão definidos "RFC 8276" e habilitados em clientes NFS modernos. Eles podem ser usados para anexar metadados definidos pelo usuário a objetos do sistema de arquivos, e são de interesse em implantações de segurança avançadas.

Atributos estendidos NFS não são atualmente suportados para operações de despejo NDMP. Se atributos estendidos forem encontrados em arquivos ou diretórios, o despejo prossegue, mas não faz backup dos atributos estendidos nesses arquivos ou diretórios.

Se você precisar desativar atributos estendidos, use o `vserver nfs modify -v4.2-xattrs disabled` comando.

Suporte ONTAP para NFS paralelo

O ONTAP dá suporte a NFS paralelo (pNFS). O protocolo pNFS oferece melhorias de desempenho ao proporcionar aos clientes acesso direto aos dados de um conjunto de arquivos distribuídos por vários nós de um cluster. Ele ajuda os clientes a localizar o caminho ideal para um volume.

Utilização de suportes rígidos

Ao solucionar problemas de montagem, você precisa ter certeza de que está usando o tipo de montagem correto. O NFS suporta dois tipos de montagem: Suportes macios e suportes rígidos. Você deve usar apenas suportes rígidos por razões de confiabilidade.

Você não deve usar montagens virtuais, especialmente quando houver possibilidade de tempos limite frequentes de NFS. As condições de corrida podem ocorrer como resultado desses tempos limite, o que pode levar à corrupção de dados.

Dependências de nomes de arquivos e diretórios NFS e SMB

Visão geral das dependências de nomes de arquivos e diretórios NFS e SMB

As convenções de nomenclatura de arquivos e diretórios dependem tanto dos sistemas operacionais dos clientes de rede quanto dos protocolos de compartilhamento de arquivos, além das configurações de idioma do cluster e dos clientes do ONTAP.

O sistema operacional e os protocolos de compartilhamento de arquivos determinam o seguinte:

- Carateres que um nome de arquivo pode usar
- Sensibilidade em caso de um nome de ficheiro

O ONTAP suporta carateres multibyte em nomes de arquivo, diretório e qtree, dependendo da versão do ONTAP.

Carateres que um nome de arquivo ou diretório pode usar

Se você estiver acessando um arquivo ou diretório de clientes com sistemas operacionais diferentes, use carateres válidos em ambos os sistemas operacionais.

Por exemplo, se você usar UNIX para criar um arquivo ou diretório, não use dois pontos (:) no nome porque os dois pontos não são permitidos em nomes de arquivo ou diretório MS-dos. Como as restrições em carateres válidos variam de um sistema operacional para outro, consulte a documentação do sistema operacional cliente para obter mais informações sobre carateres proibidos.

Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo

Os nomes de arquivos e diretórios são sensíveis a maiúsculas e minúsculas para clientes NFS, mas que preservam casos para clientes SMB. Você deve entender quais são as implicações em um ambiente multiprotocolo e as ações que pode precisar tomar ao especificar o caminho ao criar compartilhamentos SMB e ao acessar dados nos compartilhamentos.

Se um cliente SMB criar um diretório `testdir` chamado , os clientes SMB e NFS exibirão o nome do arquivo como `testdir`. No entanto, se um usuário SMB tentar criar um nome de diretório mais tarde `TESTDIR` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar posteriormente um diretório `TESTDIR` chamado , clientes NFS e SMB exibirão o nome do diretório de maneira diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de diretório à medida que foram criados, por `testdir` exemplo e `TESTDIR`, porque os nomes de diretório são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois diretórios. Um diretório tem o nome do arquivo base. Os diretórios adicionais recebem um nome de arquivo 8,3.
  - Em clientes SMB, você verá `testdir` e `TESTDI~1`.
  - O ONTAP cria o `TESTDI~1` nome do diretório para diferenciar os dois diretórios.

    Nesse caso, você deve usar o nome 8,3 ao especificar um caminho de compartilhamento ao criar ou modificar um compartilhamento em uma máquina virtual de storage (SVM).

Da mesma forma para arquivos, se um cliente SMB criar `test.txt`, os clientes SMB e NFS exibirão o nome do arquivo como `text.txt`. No entanto, se um usuário SMB tentar criar mais tarde `Test.txt` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar mais tarde um arquivo `Test.txt` chamado , clientes NFS e SMB exibirão o nome do arquivo de forma diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de arquivos à medida que foram criados e `test.txt` `Test.txt` , porque os nomes de arquivos são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois arquivos. Um arquivo tem o nome do arquivo base. Os ficheiros adicionais recebem um nome de ficheiro 8,3.
  - Em clientes SMB, você verá `test.txt` e `TEST~1.TXT`.
  - O ONTAP cria o `TEST~1.TXT` nome do arquivo para diferenciar os dois arquivos.

> Se um mapeamento de carateres tiver sido criado usando os comandos SVM CIFS de mapeamento de carateres, uma pesquisa do Windows que normalmente seria insensível a maiúsculas e minúsculas pode se tornar sensível a maiúsculas e minúsculas. Isso significa que as pesquisas de nome de arquivo só serão sensíveis a maiúsculas e minúsculas se o mapeamento de carateres tiver sido criado e o nome de arquivo estiver usando esse mapeamento de carateres.

Como o ONTAP cria nomes de arquivo e diretório

O ONTAP cria e mantém dois nomes para arquivos ou diretórios em qualquer diretório que tenha acesso de um cliente SMB: O nome longo original e um nome no formato 8,3.

Para nomes de arquivo ou diretório que excedam o nome de oito carateres ou o limite de extensão de três carateres (para arquivos), o ONTAP gera um nome de formato 8,3 da seguinte forma:

- Ele trunca o nome do arquivo ou diretório original para seis carateres, se o nome exceder seis carateres.
- Ele adiciona um til (…) e um número, um a cinco, aos nomes de arquivo ou diretório que não são mais exclusivos depois de serem truncados.

  Se ele ficar sem números porque há mais de cinco nomes semelhantes, ele cria um nome exclusivo que não tem relação com o nome original.

- No caso dos arquivos, ele trunca a extensão do nome do arquivo para três carateres.

Por exemplo, se um cliente NFS criar um arquivo chamado `specifications.html`, o nome do arquivo de formato 8,3 criado pelo ONTAP será `specif~1.htm`. Se esse nome já existir, o ONTAP usará um número diferente no final do nome do arquivo. Por exemplo, se um cliente NFS criar outro arquivo chamado `specifications_new.html`, o formato 8,3 do `specifications_new.html` é `specif~2.htm`.

Como o ONTAP lida com nomes de arquivos, diretórios e qtree de vários bytes

Começando com ONTAP 9.5, o suporte para nomes codificados UTF-8 de 4 bytes permite a criação e exibição de nomes de arquivos, diretórios e árvores que incluem carateres suplementares Unicode fora do plano multilíngue básico (BMP). Em versões anteriores, esses carateres suplementares não foram exibidos corretamente em ambientes multiprotocolo.

Para ativar o suporte para nomes codificados UTF-8 de 4 bytes, um novo código de linguagem *utf8mb4* está disponível para as `vserver` famílias de comandos e `volume` .

- Você deve criar um novo volume de uma das seguintes maneiras:
- Definir a opção de volume `-language` explicitamente:

  ```
  volume create -language utf8mb4 {…}
  ```

- Herdando a opção de volume `-language` de uma SVM que foi criada ou modificada para a opção:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Se você estiver usando o ONTAP 9.6 e anteriores, não será possível modificar volumes existentes para suporte a utf8mb4; você deve criar um novo volume pronto para utf8mb4 e migrar os dados usando ferramentas de cópia baseadas em cliente.

  Se você estiver usando o ONTAP 9.7P1 ou posterior, poderá modificar volumes existentes para o utf8mb4 com uma solicitação de suporte. Para obter mais informações, "O idioma do volume pode ser alterado após a criação no ONTAP?"consulte .

Você pode atualizar SVMs para suporte a utf8mb4, mas os volumes existentes mantêm seus códigos de idioma originais.

E

Nomes LUN com carateres UTF-8 de 4 bytes não são suportados atualmente.

- Os dados de carateres Unicode são normalmente representados em aplicações de sistemas de ficheiros Windows utilizando o formato de transformação Unicode de 16 bits (UTF-16) e em sistemas de ficheiros NFS utilizando o formato de transformação Unicode de 8 bits (UTF-8).

  Em versões anteriores ao ONTAP 9.5, nomes incluindo carateres suplementares UTF-16 que foram criados por clientes Windows foram exibidos corretamente para outros clientes Windows, mas não foram traduzidos corretamente para UTF-8 para clientes NFS. Da mesma forma, nomes com carateres suplementares UTF-8 por clientes NFS criados não foram traduzidos corretamente para UTF-16 para clientes Windows.

- Quando você cria nomes de arquivo em sistemas que executam o ONTAP 9.4 ou anteriores que contêm carateres suplementares válidos ou inválidos, o ONTAP rejeita o nome do arquivo e retorna um erro de nome de arquivo inválido.

  Para evitar esse problema, use apenas carateres BMP em nomes de arquivo e evite usar carateres suplementares ou atualize para o ONTAP 9.5 ou posterior.

Carateres Unicode são permitidos em nomes de qtree.

- Você pode usar a `volume qtree` família de comandos ou o System Manager para definir ou modificar nomes de qtree.
- Os nomes de qtree podem incluir carateres de vários bytes no formato Unicode, como carateres japoneses e chineses.
- Em versões anteriores ao ONTAP 9.5, apenas os carateres BMP (ou seja, aqueles que poderiam ser representados em 3 bytes) foram suportados.

Em versões anteriores ao ONTAP 9.5, o caminho de junção do volume pai da qtree pode conter nomes de qtree e diretório com carateres Unicode. O `volume show` comando exibe esses nomes corretamente quando o volume pai tem uma configuração de idioma UTF-8. No entanto, se o idioma do volume pai não for uma das configurações de idioma UTF-8, algumas partes do caminho de junção serão exibidas usando um nome alternativo NFS numérico.

- Em versões 9,5 e posteriores, os carateres de 4 bytes são suportados em nomes de qtree, desde que a qtree esteja em um volume habilitado para utf8mb4.

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Os clientes NFS podem criar nomes de arquivos que contêm carateres que não são válidos para clientes SMB e determinados aplicativos do Windows. Você pode configurar o mapeamento de carateres para a tradução de nome de arquivo em volumes para permitir que clientes SMB acessem arquivos com nomes NFS que, de outra forma, não seriam válidos.

Sobre esta tarefa

Quando os arquivos criados por clientes NFS são acessados por clientes SMB, o ONTAP examina o nome do arquivo. Se o nome não for um nome de arquivo SMB válido (por exemplo, se ele tiver um caractere de dois pontos "':'" incorporado), o ONTAP retornará o nome de arquivo 8,3 que é mantido para cada arquivo. No entanto, isso causa problemas para aplicativos que codificam informações importantes em nomes de arquivos longos.

Portanto, se você estiver compartilhando um arquivo entre clientes em sistemas operacionais diferentes, você deve usar carateres nos nomes de arquivo que são válidos em ambos os sistemas operacionais.

No entanto, se você tiver clientes NFS que criam nomes de arquivo contendo carateres que não são nomes de arquivo válidos para clientes SMB, você poderá definir um mapa que converte os carateres NFS inválidos em carateres Unicode que tanto SMB quanto determinados aplicativos do Windows aceitam. Por exemplo, essa funcionalidade suporta os aplicativos CATIA MCAD e Mathematica, bem como outros aplicativos que têm esse requisito.

Você pode configurar o mapeamento de carateres em uma base volume por volume.

Você deve ter em mente o seguinte ao configurar o mapeamento de carateres em um volume:

- O mapeamento de carateres não é aplicado em pontos de junção.

  Você deve configurar explicitamente o mapeamento de carateres para cada volume de junção.

- Você deve certificar-se de que os carateres Unicode que são usados para representar carateres inválidos ou ilegais são carateres que normalmente não aparecem em nomes de arquivos; caso contrário, mapeamentos indesejados ocorrem.

  Por exemplo, se você tentar mapear dois pontos (:) para um hífen (-), mas o hífen (-) foi usado no nome do arquivo corretamente, um cliente Windows tentando acessar um arquivo chamado "'a-b'" teria sua solicitação mapeada para o nome NFS de "'a:b'" (não o resultado desejado).

- Depois de aplicar o mapeamento de carateres, se o mapeamento ainda contiver um caractere Windows inválido, o ONTAP volta para os nomes de arquivos do Windows 8,3.

- Em notificações FPolicy, logs de auditoria nas e mensagens de rastreamento de segurança, os nomes de arquivo mapeados são exibidos.
- Quando uma relação SnapMirror do tipo DP é criada, o mapeamento de carateres do volume de origem não é replicado no volume DP de destino.
- Sensibilidade do caso: Como os nomes mapeados do Windows se transformam em nomes NFS, a pesquisa dos nomes segue semântica de NFS. Isso inclui o fato de que pesquisas NFS são sensíveis a maiúsculas e minúsculas. Isso significa que os aplicativos que acessam compartilhamentos mapeados não devem depender de comportamento insensível a maiúsculas e minúsculas do Windows. No entanto, o nome 8,3 está disponível, e isso é insensível a maiúsculas e minúsculas.
- Mapeamentos parciais ou inválidos: Depois de mapear um nome para retornar aos clientes fazendo enumeração de diretórios ("dir"), o nome Unicode resultante é verificado para a validade do Windows. Se esse nome ainda tiver carateres inválidos nele, ou se for inválido para o Windows (por exemplo, termina em "." ou em branco), o nome 8,3 será retornado em vez do nome inválido.

Passo

1. Configurar mapeamento de carateres:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   O mapeamento consiste em uma lista de pares de carateres fonte-alvo separados por "':'". Os carateres são carateres Unicode inseridos usando dígitos hexadecimais. Por exemplo: 3c:E03C.

   O primeiro valor de cada `mapping_text` par que é separado por dois pontos é o valor hexadecimal do caractere NFS que você deseja traduzir, e o segundo valor é o valor Unicode que SMB usa. Os pares de mapeamento devem ser únicos (deve existir um mapeamento um-para-um).

   - Mapeamento de origem

     A tabela a seguir mostra o conjunto de carateres Unicode permissível para mapeamento de fontes:

Caractere Unicode	Caráter impresso	Descrição
0x01-0x19	Não aplicável	Caracteres de controle não-impressão
0x5C	*	Barra invertida
0x3A	:	Cólon
0x2A	*	Asterisco
0x3F	?	Ponto de interrogação
0x22	"	Marca de cotação
0x3C	*	Menos de
0x3E	>	Superior a.

0x7C		
Linha vertical	0xB1	±

- Mapeamento de alvos

  Você pode especificar carateres de destino na ""Área de uso privado"" do Unicode no seguinte intervalo: U-E0000…U-F8FF.

Exemplo

O comando a seguir cria um mapeamento de carateres para um volume chamado "data" na máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Comandos para gerenciar mapeamentos de carateres para a tradução de nome de arquivo SMB

É possível gerenciar o mapeamento de carateres criando, modificando, exibindo informações ou excluindo mapeamentos de carateres de arquivo usados para a tradução de nomes de arquivo SMB em volumes FlexVol.

Se você quiser…	Use este comando…
Criar novos mapeamentos de carateres de arquivo	`vserver cifs character-mapping create`
Exibir informações sobre mapeamentos de carateres de arquivo	`vserver cifs character-mapping show`
Modificar mapeamentos de carateres de arquivo existentes	`vserver cifs character-mapping modify`
Excluir mapeamentos de carateres de arquivo	`vserver cifs character-mapping delete`

Para obter mais informações, consulte a página man para cada comando.

Gerenciar trunking NFS

Saiba mais sobre o entroncamento do ONTAP NFS

A partir do ONTAP 9.14,1, os clientes NFSv4,1 podem aproveitar o entroncamento de sessão para abrir várias conexões a diferentes LIFs no servidor NFS, aumentando assim a velocidade de transferência de dados e fornecendo resiliência por meio de multipathing.

O entroncamento é vantajoso para exportar volumes FlexVol para clientes com capacidade de entroncamento, em particular clientes VMware e Linux, ou para NFS sobre RDMA, TCP ou pNFS.

No ONTAP 9.14,1, o entroncamento é restrito a LIFs em um único nó; o entroncamento não pode abranger LIFs em vários nós.

Os volumes FlexGroup são compatíveis com o entroncamento. Embora isso possa proporcionar melhor desempenho, o acesso multipath a um volume FlexGroup só pode ser configurado em um único nó.

Somente o entroncamento de sessão é suportado para multipathing nesta versão.

Como usar o entroncamento

Para aproveitar os benefícios de vários pathing oferecidos pelo entroncamento, você precisa de um conjunto de LIFs – conhecido como *entroncamento group* – que esteja associado ao SVM que contém um servidor NFS habilitado para entroncamento. Os LIFs em um grupo de entroncamento devem ter portas home no mesmo nó do cluster e devem residir nessas portas home. É uma prática recomendada que todos os LIFs de um grupo de entroncamento sejam membros do mesmo grupo de failover.

O ONTAP suporta até 16 conexões truncadas por nó de um determinado cliente.

Quando um cliente monta exportações de um servidor habilitado para entroncamento, ele especifica um número de endereços IP para LIFs em um grupo de entroncamento. Depois que o cliente se coneta ao primeiro LIF, LIFs adicionais só são adicionados à sessão NFSv4,1 e usados para entroncamento se eles estiverem em conformidade com os requisitos do grupo de entroncamento. Em seguida, o cliente distribui operações NFS pelas várias conexões com base em seu próprio algoritmo (como round-robin).

Para obter a melhor performance, configure o entroncamento em uma SVM dedicada a fornecer exportações de multipath, e não exportações de caminho único. Ou seja, você só deve habilitar o entroncamento em um servidor NFS em um SVM cujas exportações são fornecidas apenas para clientes habilitados para entroncamento.

Clientes suportados

O servidor ONTAP NFSv4,1 suporta entroncamento com qualquer cliente capaz de entroncamento de sessão NFSv4,1.

Os seguintes clientes foram testados com o ONTAP 9.14,1:

- VMware - ESXi 7.0U3F e posterior
- Linux - Red Hat Enterprise Linux (RHEL) 8,8 e 9,3

Quando o entroncamento é ativado em um servidor NFS, os usuários que acessam compartilhamentos exportados em clientes NFS que não suportam entroncamento podem ver uma queda de desempenho. Isso ocorre porque apenas uma única conexão TCP é usada para várias montagens nos LIFs de dados da SVM.

Diferença entre o entroncamento NFS e o nconnect

A partir do ONTAP 9.8, a funcionalidade nconnect está disponível por predefinição quando o NFSv4,1 está ativado. Em clientes compatíveis com nconnect, uma única montagem NFS pode ter várias conexões TCP (até 16) em um único LIF.

Em contraste, o entroncamento é a funcionalidade *multipathing*, que fornece várias conexões TCP sobre vários LIFs. Se você tiver a capacidade de empregar NICs adicionais em seu ambiente, o entroncamento fornece maior paralelismo e desempenho além da capacidade do nconnect.

Saiba mais sobre "nligar."

Configurar um novo servidor NFS e exportar para entroncamento

Criar um servidor NFS habilitado para trunking em um SVM do ONTAP

A partir do ONTAP 9.14,1, o entroncamento pode ser ativado em servidores NFS. O NFSv4,1 é ativado por padrão quando os servidores NFS são criados.

Antes de começar

A criação de um servidor NFS habilitado para trunking requer uma SVM. O SVM precisa ser:

- apoiado por armazenamento suficiente para os requisitos de dados do cliente.
- Habilitado para NFS.

Você pode usar uma SVM existente. No entanto, a ativação do entroncamento requer que todos os clientes NFSv4.x sejam remontados, o que pode ser disruptivo. Se não for possível montar novamente, crie um novo SVM para o servidor NFS.

Passos

1. Se não houver um SVM adequado, crie um:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Verifique a configuração e o status do SVM recém-criado:

   ```
   vserver show -vserver svm_name
   ```

   Saiba mais "Criação de um SVM"sobre o .

3. Crie o servidor NFS:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Verifique se o NFS está em execução:

```
vserver nfs status -vserver svm_name
```

5. Verifique se o NFS está configurado conforme desejado:

```
vserver nfs show -vserver svm_name
```

Saiba mais sobre "Configuração do servidor NFS."

Depois de terminar

Configure os seguintes serviços conforme necessário:

- "DNS"
- "LDAP"
- "Kerberos"

Prepare sua rede para o entroncamento de NFS do ONTAP

Para aproveitar o entroncamento NFSv4,1, os LIFs em um grupo de entroncamento devem residir no mesmo nó e ter portas iniciais no mesmo nó. As LIFs devem ser configuradas em um grupo de failover no mesmo nó.

Sobre esta tarefa

Um mapeamento individual de LIFs e NICs produz o maior ganho de desempenho, mas não é necessário para habilitar o entroncamento. Ter pelo menos duas NICs instaladas pode oferecer um benefício de desempenho, mas não é necessário.

Você pode ter vários grupos de failover, mas o grupo de failover para o entroncamento deve incluir apenas os LIFS no grupo de entroncamento.

Você deve ajustar o grupo de failover do entroncamento sempre que adicionar ou remover conexões (e NICs subjacentes) de um grupo de failover.

Antes de começar

- Você deve saber os nomes das portas associadas às placas de rede se quiser criar um grupo de failover.
- Todas as portas devem estar no mesmo nó.

Passos

1. Verifique os nomes e o status das portas de rede que você planeja usar:

```
network port status
```

2. Crie o grupo failover:

```
network interface failover-groups create -vserver svm_name -failover-group
failover_group_name -targets ports_list
```

> Não é um requisito ter um grupo de failover, mas é altamente recomendável.

   - *svm_name* É o nome do SVM que contém o servidor NFS.
   - *ports_list* é a lista de portas que serão adicionadas ao grupo failover.

As portas são adicionadas no formato *node_name:port_number*, por exemplo, node1:e0c.

O comando a seguir cria o grupo de failover FG3 para SVM VS1 e adiciona três portas:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Saiba mais sobre "grupos de failover."

3. Se necessário, crie LIFs para membros do grupo de entroncamento:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

   - `-home-node` - O nó para o qual o LIF retorna quando o comando de reversão de interface de rede é executado no LIF.

     Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

   - `-home-port` É a porta física ou lógica à qual o LIF retorna quando o comando de reversão da interface de rede é executado no LIF.
   - Pode especificar um endereço IP com `-address` as opções e `-netmask`, não com a `-subnet` opção.
   - Quando você atribui endereços IP, talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
   - `-service-policy` - A política de serviços para o LIF. Se nenhuma política for especificada, uma política padrão será atribuída automaticamente. Use o `network interface service-policy show` comando para revisar as políticas de serviço disponíveis.
   - `-auto-revert` - Especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é falsa, mas você pode configurá-la como verdadeira dependendo das políticas de gerenciamento de rede em seu ambiente.

     Repita esta etapa para cada LIF no grupo de entroncamento.

     O comando a seguir cria `lif-A` para o SVM `vs1`, na porta `e0c` do nó `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Saiba mais sobre "Criação de LIF."

4. Verifique se os LIFs foram criados:

```
network interface show
```

5. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Crie uma política de exportação de volume ONTAP

Para fornecer acesso de cliente a compartilhamentos de dados, você deve criar um ou mais volumes e o volume deve ter políticas de exportação com pelo menos uma regra.

Requisitos de exportação do cliente:

- Os clientes Linux devem ter uma montagem separada e um ponto de montagem separado para cada conexão de entroncamento (ou seja, para cada LIF).
- Os clientes VMware exigem apenas um único ponto de montagem para um volume exportado, com várias LIFs especificadas.

  Os clientes VMware exigem acesso root na política de exportação.

Passos

1. Criar uma política de exportação:

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   O nome da política pode ter até 256 carateres.

2. Verifique se a política de exportação foi criada:

   ```
   vserver export-policy show -policyname policy_name
   ```

   Exemplo

   Os comandos a seguir criam e verificam a criação de uma política de exportação chamada exp1 no SVM chamado VS1:

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. Crie uma regra de exportação e adicione-a a uma política de exportação existente:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   O `-clientmatch` parâmetro deve identificar os clientes Linux ou VMware compatíveis com entroncamento que montarão a exportação.

   Saiba mais sobre "criando regras de exportação."

4. Crie o volume com um ponto de junção:

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   ```

```
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

Saiba mais "criando volumes."

5. Verifique se o volume foi criado com o ponto de junção desejado:

```
volume show -vserver svm_name -volume volume_name -junction-path
```

Montar volumes ONTAP ou compartilhamentos de dados para trunking NFS

Os clientes Linux e VMware que oferecem suporte ao entroncamento podem montar volumes ou compartilhamentos de dados de um servidor ONTAP NFSv4,1 habilitado para entroncamento.

Ao inserir comandos de montagem nos clientes, você deve inserir endereços IP para cada LIF no grupo de entroncamento.

Saiba mais "clientes suportados"sobre .

Requisitos do cliente Linux

Um ponto de montagem separado é necessário para cada conexão no grupo de entroncamento.

Monte os volumes exportados com comandos semelhantes aos seguintes:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

O (`vers`valor da versão) deve ser `4.1` ou posterior.

O `max_connect` valor corresponde ao número de conexões no grupo de entroncamento.

Requisitos do cliente VMware

É necessário um comando mount que inclua um endereço IP para cada conexão no grupo de entroncamento.

Monte o datastore exportado com um comando semelhante ao seguinte:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Os `-H` valores correspondem às conexões no grupo entroncamento.

Adaptar as exportações de NFS existentes para o trunking

Adaptar exportações de caminho único para o entroncamento de NFS da ONTAP

Você pode adaptar uma exportação NFSv4,1 de caminho único existente (não truncado) para usar o entroncamento. Os clientes com capacidade para entroncamento podem

aproveitar o desempenho melhorado assim que o entroncamento é ativado no servidor, desde que os pré-requisitos do servidor e do cliente tenham sido satisfeitos.

Adaptar uma exportação de caminho único para o entroncamento permite manter conjuntos de dados exportados em seus volumes e SVMs existentes. Para fazer isso, você deve habilitar o entroncamento no servidor NFS, atualizar a configuração de rede e exportar e remontar o compartilhamento exportado nos clientes.

Ativar o entroncamento tem o efeito de reiniciar o servidor. Os clientes VMware devem remontar os datastores exportados; os clientes Linux devem remontar os volumes exportados com a `max_connect` opção.

Ativar o entroncamento em um servidor ONTAP NFS

O entroncamento deve ser explicitamente ativado em servidores NFS. O NFSv4,1 é ativado por padrão quando os servidores NFS são criados.

Depois de ativar o entroncamento, verifique se os seguintes serviços estão configurados conforme necessário.

- "DNS"
- "LDAP"
- "Kerberos"

Passos

1. Ative o entroncamento e certifique-se de que o NFSv4,1 está ativado:

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Verifique se o NFS está em execução:
   ```
   vserver nfs status -vserver svm_name
   ```
3. Verifique se o NFS está configurado conforme desejado:

   ```
   vserver nfs show -vserver svm_name
   ```

   Saiba mais sobre "Configuração do servidor NFS.".. Se você estiver atendendo a clientes Windows a partir deste SVM, mova os compartilhamentos e exclua o servidor.
   ```
   vserver cifs show -vserver svm_name
   ```

   E
   ```
   vserver cifs delete -vserver svm_name
   ```

Atualize sua rede para o entroncamento de NFS do ONTAP

O entroncamento NFSv4,1 exige que os LIFs em um grupo de entroncamento residam no mesmo nó e tenham portas iniciais no mesmo nó. Todas as LIFs devem ser configuradas em um grupo de failover no mesmo nó.

Sobre esta tarefa

Um mapeamento individual de LIFs e NICs produz o maior ganho de desempenho, mas não é necessário para habilitar o entroncamento.

Você pode ter vários grupos de failover, mas o grupo de failover para o entroncamento deve incluir apenas os LIFS no grupo de entroncamento.

Você deve ajustar o grupo de failover do entroncamento sempre que adicionar ou remover conexões (e NICs subjacentes) de um grupo de failover.

Antes de começar

- Você deve saber os nomes das portas associadas às placas de rede para criar um grupo de failover.
- Todas as portas devem estar no mesmo nó.

Passos

1. Verifique os nomes e o status das portas de rede que você planeja usar:

   ```
   network port show
   ```

2. Crie um grupo de failover de entroncamento ou modifique um grupo existente para entroncamento:

   ```
   network interface failover-groups create -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

   ```
   network interface failover-groups modify -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

   Não é um requisito ter um grupo de failover, mas é altamente recomendável.

   - *svm_name* É o nome do SVM que contém o servidor NFS.
   - *ports_list* é a lista de portas que serão adicionadas ao grupo failover.

     As portas são adicionadas no formato *node_name:port_number*, por exemplo `node1:e0c`, .

     O comando a seguir cria um grupo de failover `fg3` para o SVM VS1 e adiciona três portas:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   Saiba mais sobre "grupos de failover."

3. Crie LIFs adicionais para membros do grupo de entroncamento conforme necessário:

   ```
   network interface create -vserver svm_name -lif lif_name -home-node node_name
   -home-port port_name -address IP_address -netmask IP_address [-service-policy
   policy] [-auto-revert {true|false}]
   ```

   - `-home-node` - O nó para o qual o LIF retorna quando o comando de reversão de interface de rede é executado no LIF.

     Você pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

   - `-home-port` É a porta física ou lógica à qual o LIF retorna quando o comando de reversão da interface de rede é executado no LIF.

- Pode especificar um endereço IP com `-address` as opções e. `-netmask`
- Quando você atribui endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A página de manual de criação de rota de rede contém informações sobre a criação de uma rota estática em um SVM.
- `-service-policy` - A política de serviços para o LIF. Se nenhuma política for especificada, uma política padrão será atribuída automaticamente. Use o `network interface service-policy show` comando para revisar as políticas de serviço disponíveis.
- `-auto-revert` - Especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. **A configuração padrão é FALSE**, mas você pode configurá-la como verdadeira dependendo das políticas de gerenciamento de rede em seu ambiente.

  Repita esta etapa para cada LIF adicional necessário no grupo de entroncamento.

  O comando a seguir cria lif-A para o SVM VS1, na porta e0c do nó cluster1_01:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

Saiba mais sobre "Criação de LIF."

4. Verifique se os LIFs foram criados:

   ```
   network interface show
   ```

5. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Modificar políticas de exportação de volume ONTAP

Para permitir que os clientes aproveitem o entroncamento para compartilhamentos de dados existentes, talvez seja necessário modificar políticas e regras de exportação e os volumes aos quais estão anexados. Existem diferentes requisitos de exportação para clientes Linux e datastores VMware.

Requisitos de exportação do cliente:

- Os clientes Linux devem ter uma montagem separada e um ponto de montagem separado para cada conexão de entroncamento (ou seja, para cada LIF).

  Se você estiver atualizando para o ONTAP 9.14,1 e já tiver exportado um volume, poderá continuar a usar esse volume em um grupo de entroncamento.

- Os clientes VMware exigem apenas um único ponto de montagem para um volume exportado, com várias LIFs especificadas.

Os clientes VMware exigem acesso root na política de exportação.

Passos

1. Verifique se uma política de exportação existente está em vigor:

   ```
   vserver export-policy show
   ```

2. Verifique se as regras de política de exportação existentes são apropriadas para a configuração do entroncamento:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   Em particular, verifique se o `-clientmatch` parâmetro identifica corretamente os clientes Linux ou VMware compatíveis com entroncamento que montarão a exportação.

   Se forem necessários ajustes, modifique a regra usando o `vserver export-policy rule modify` comando ou crie uma nova regra:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Saiba mais sobre "criando regras de exportação."

3. Verifique se os volumes exportados existentes estão online:

   ```
   volume show -vserver svm_name
   ```

Remontagem de volumes de ONTAP ou compartilhamentos de dados para trunking NFS

Para converter conexões de cliente não truncadas em conexões truncadas, as montagens existentes nos clientes Linux e VMware devem ser desmontadas e remontadas usando informações sobre LIFs.

Ao inserir comandos de montagem nos clientes, você deve inserir endereços IP para cada LIF no grupo de entroncamento.

Saiba mais "clientes suportados"sobre .

> A desinstalação de clientes VMware causa interrupções em todas as VMs no datastore. Uma alternativa seria criar um novo datastore habilitado para entroncamento e usar **Storage vmotion** para mover suas VMs do datastore antigo para o novo. Consulte a documentação da VMware para obter detalhes.

Requisitos do cliente Linux

Um ponto de montagem separado é necessário para cada conexão no grupo de entroncamento.

Monte os volumes exportados com comandos semelhantes aos seguintes:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

O `vers` valor deve ser `4.1` ou posterior.

O `max_connect` valor deve corresponder ao número de conexões no grupo de entroncamento.

Requisitos do cliente VMware

É necessário um comando mount que inclua um endereço IP para cada conexão no grupo de entroncamento.

Monte o datastore exportado com um comando semelhante ao seguinte:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Os `-H` valores devem corresponder às conexões no grupo de entroncamento.

Gerenciar NFS em RDMA

Visão geral de NFS sobre RDMA

O NFS sobre RDMA utiliza adaptadores RDMA, permitindo que os dados sejam copiados diretamente entre a memória do sistema de armazenamento e a memória do sistema host, contornando as interrupções da CPU e a sobrecarga.

As configurações NFS sobre RDMA são projetadas para clientes com workloads sensíveis à latência ou com alta largura de banda, como machine learning e análises. A NVIDIA estendeu o NFS por RDMA para habilitar o armazenamento direto da GPU (GDS). O GDS acelera ainda mais as cargas de trabalho com GPU, ignorando completamente a CPU e a memória principal, usando RDMA para transferir dados entre o sistema de armazenamento e a memória GPU diretamente.

A partir do ONTAP 9.10,1, as configurações NFS sobre RDMA são suportadas para o protocolo NFSv4,0 quando usado com o adaptador Mellanox CX-5 ou CX-6, que fornece suporte para RDMA usando a versão 2 do protocolo RoCE. O GDS só é suportado usando GPUs da família NVIDIA Tesla e Ampere com placas de rede Mellanox e software MOFED. Consulte o gráfico em requisitos para entender o suporte à versão NFS nas versões subsequentes do ONTAP.

Tamanhos de montagem de NFS maiores que 64k mm resultam em desempenho instável com configurações NFS em RDMA.

Requisitos

- Os sistemas de armazenamento devem estar executando o ONTAP 9.10,1 ou posterior.
- Certifique-se de que está a executar a versão correta do ONTAP para a versão NFS que pretende utilizar.

Versão de NFS	Suporte à ONTAP
NFSv4.0	ONTAP 9.10,1 e posterior
NFSv4.1	ONTAP 9.14,1 e posterior
NFSv3	ONTAP 9.15,1 e posterior

    - Você pode configurar o NFS através do RDMA com o Gerenciador de sistemas a partir do ONTAP 9.12,1. No ONTAP 9.10,1 e 9.11.1, você precisa usar a CLI para configurar o NFS em RDMA.
- Ambos os nós no par de HA devem ter a mesma versão.
- Os controladores do sistema de storage devem ter suporte a RDMA

Começando em ONTAP…	Os seguintes controladores suportam RDMA…
9.10.1 e mais tarde	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14,1 e posterior	• Série C da AFF • AFF A900
ONTAP 9.15,1 e posterior	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16,1 e posterior	• AFF A50 • AFF A30 • AFF A20

- As LIFs de dados devem ser configuradas para suportar RDMA.
- Os clientes devem estar usando placas NIC compatíveis com RDMA Mellanox e software de rede Mellanox OFED (MOFED). Para obter informações sobre o suporte do adaptador, consulte o "NetApp Hardware Universe". Os adaptadores compatíveis com NFS sobre RDMA exibem "RoCE" no campo de descrição.

Os grupos de interfaces não são compatíveis com NFS em RDMA.

Próximas etapas

- Configurar NICs para NFS em RDMA
- Configurar LIFs para NFS em RDMA
- Configurações de NFS para NFS em RDMA

Informações relacionadas

- "RDMA"
- Visão geral do trunking NFS

- "RFC 7530: Protocolo NFS versão 4"
- "RFC 8166: Transporte remoto de acesso direto à memória para chamada de procedimento remoto versão 1"
- "RFC 8167: Chamada de procedimento remoto bidirecional em transportes RPC-over-RDMA"
- "RFC 8267: Vinculação de camada superior NFS para RPC-over-RDMA versão 1"

Configurar NICs para NFS em RDMA

O NFS sobre RDMA requer configuração de NIC para o sistema cliente e plataforma de armazenamento.

Configuração da plataforma de storage

Um adaptador RDMA X1148 precisa ser instalado no servidor. Se você estiver usando uma configuração de HA, precisará ter um adaptador X1148 correspondente no parceiro de failover para que o serviço RDMA possa continuar durante o failover. A NIC deve ser compatível com ROCE.

A partir do ONTAP 9.10,1, você pode visualizar uma lista de protocolos de descarga RDMA com o comando: `network port show -rdma-protocols roce`

Configuração do sistema cliente

Os clientes devem estar usando placas NIC compatíveis com RDMA Mellanox (por exemplo, X1148) e software de rede Mellanox OFED. Consulte a documentação do Mellanox para ver os modelos e versões compatíveis. Embora o cliente e o servidor possam ser conetados diretamente, o uso de switches é recomendado devido ao melhor desempenho de failover com um switch.

O cliente, o servidor, todos os switches e todas as portas nos switches devem ser configurados usando Jumbo Frames. Certifique-se também de que o controle de fluxo de prioridade está em vigor em quaisquer switches.

Depois que essa configuração for confirmada, você poderá montar o NFS.

System Manager

Você deve estar usando o ONTAP 9.12,1 ou posterior para configurar interfaces de rede com o NFS através do RDMA usando o Gerenciador de sistemas.

Passos

1. Verifique se o RDMA é suportado. Navegue até **rede > portas Ethernet** e selecione o nó apropriado na exibição de grupo. Quando você expandir o nó, observe o campo **protocolos RDMA** para uma determinada porta: O valor **RoCE** indica que RDMA é suportado; um traço (**-**) indica que não é suportado.
2. Para adicionar uma VLAN, selecione * VLAN*. Selecione o nó apropriado. No menu suspenso **Port**, as portas disponíveis exibem o texto **RoCE Enabled** se suportarem RDMA. Nenhum texto é exibido se eles não suportarem RDMA.
3. Siga o fluxo de trabalho em Ative o storage nas para servidores Linux usando NFS para configurar um novo servidor NFS.

   Ao adicionar interfaces de rede, você terá a opção de selecionar **usar portas RoCE**. Selecione esta opção para todas as interfaces de rede que você deseja usar NFS sobre RDMA.

CLI

1. Verifique se o acesso RDMA está ativado no servidor NFS com o comando:

   ```
   vserver nfs show-vserver SVM_name
   ```

   Por padrão, `-rdma` deve estar habilitado. Se não estiver, ative o acesso RDMA no servidor NFS:

   ```
   vserver nfs modify -vserver SVM_name -rdma enabled
   ```

2. Monte o cliente via NFSv4,0 através de RDMA:
   a. A entrada para o parâmetro proto depende da versão do protocolo IP do servidor. Se for IPv4, use `proto=rdma`. Se for IPv6, use `proto=rdma6`.
   b. Especifique a porta de destino NFS como `port=20049` em vez da porta padrão 2049:

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address
   :/volume_path mount_point
   ```

3. **OPCIONAL**: Se você precisar desmontar o cliente, execute o comando `unmount mount_path`

Mais informações

- Crie um servidor NFS
- Ative o storage nas para servidores Linux usando NFS

Configurar LIFs para NFS em RDMA

Para utilizar NFS sobre RDMA, você deve configurar seus LIFs (interface de rede) para serem compatíveis com RDMA. Tanto o LIF quanto seu par de failover devem ser capazes de suportar RDMA.

Crie um novo LIF

System Manager

Você deve estar executando o ONTAP 9.12,1 ou posterior para criar uma interface de rede para NFS através do RDMA com o Gerenciador de sistemas.

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. + Add Selecione .
3. Quando você seleciona **NFS, SMB/CIFS,S3**, você tem a opção **usar portas RoCE**. Marque a caixa de seleção **Use RoCE Ports**.
4. Selecione a VM de armazenamento e o nó inicial. Atribua um **Nome**, **endereço IP** e **máscara de sub-rede**.
5. Depois de inserir o endereço IP e a máscara de sub-rede, o System Manager filtra a lista de domínios de broadcast para aqueles que têm portas compatíveis com RoCE. Selecione um domínio de broadcast. Opcionalmente, você pode adicionar um gateway.
6. Selecione **Guardar**.

CLI

Passos

1. Criar um LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - A política de serviço deve ser arquivos de dados padrão ou uma política personalizada que inclua o serviço de interface de rede data nfs.
   - O `-rdma-protocols` parâmetro aceita uma lista, que é por padrão vazia. Quando `roce` é adicionado como um valor, o LIF só pode ser configurado em portas que suportam descarga RoCE, afetando a migração de bot LIF e o failover.

Modificar um LIF

System Manager

Você deve estar executando o ONTAP 9.12,1 ou posterior para criar uma interface de rede para NFS através do RDMA com o Gerenciador de sistemas.

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione **> Editar** ao lado da interface de rede que deseja alterar.
3. Marque **Use RoCE Ports** para habilitar o NFS em RDMA ou desmarque a caixa para desativá-lo. Se a interface de rede estiver em uma porta compatível com RoCE, você verá uma caixa de seleção ao lado de **usar portas RoCE**.
4. Modifique as outras definições conforme necessário.
5. Selecione **Salvar** para confirmar suas alterações.

CLI

1. Você pode verificar o status de seus LIFs com o `network interface show` comando. A política de serviço deve incluir o serviço de interface de rede data nfs. A `-rdma-protocols` lista deve incluir `roce`. Se qualquer uma dessas condições não for verdadeira, modifique o LIF.
2. Para modificar o LIF, execute:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

Modificar um LIF para exigir um determinado protocolo de descarga quando o LIF não está atualmente atribuído a uma porta que suporte esse protocolo produzirá um erro.

Migração de um LIF

O ONTAP também permite migrar interfaces de rede (LIFs) para utilizar o NFS em RDMA. Ao executar essa migração, você deve garantir que a porta de destino seja compatível com RoCE. A partir do ONTAP 9.12,1, pode concluir este procedimento no Gestor de sistema. Ao selecionar uma porta de destino para a interface de rede, o System Manager designará se as portas são compatíveis com RoCE.

Você só pode migrar um LIF para uma configuração NFS por RDMA se:

- É uma interface de rede NFS RDMA (LIF) hospedada em uma porta compatível com RoCE.
- É uma interface de rede TCP NFS (LIF) hospedada em uma porta compatível com RoCE.
- É uma interface de rede TCP NFS (LIF) hospedada em uma porta não compatível com RoCE.

Para obter mais informações sobre como migrar uma interface de rede, Migração de um LIFconsulte .

Mais informações

- Crie um LIF
- Crie um LIF
- Modificar um LIF

- Migração de um LIF

Modificar a configuração NFS

Na maioria dos casos, você não precisa modificar a configuração da VM de storage habilitada por NFS para NFS em RDMA.

Se você está, no entanto, lidando com problemas relacionados a chips de Mellanox e migração de LIF, você deve aumentar o período de graça de bloqueio de NFSv4. Por padrão, o período de carência é definido como 45 segundos. A partir de ONTAP 9.10,1, o período de carência tem um valor máximo de 180 (segundos).

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

Para obter mais informações sobre esta tarefa, Especifique o período de tolerância de bloqueio NFSv4consulte .

Configure o SMB com a CLI

Visão geral da configuração SMB com a CLI

Você pode usar os comandos de CLI do ONTAP 9 para configurar o acesso de cliente SMB a arquivos contidos em um novo volume ou qtree em um SVM novo ou existente.

> *SMB* (bloco de mensagens de servidor) refere-se aos dialetos modernos do protocolo Common Internet File System (CIFS). Você ainda verá *CIFS* na interface de linha de comando (CLI) do ONTAP e nas ferramentas de gerenciamento do OnCommand.

Use estes procedimentos se quiser configurar o acesso SMB a um volume ou qtree da seguinte maneira:

- Você deseja usar SMB versão 2 ou posterior.
- Você deseja atender apenas clientes SMB, não clientes NFS (não uma configuração multiprotocolo).
- As permissões de arquivo NTFS serão usadas para proteger o novo volume.
- Você tem o administrador de clusters Privileges, e não o Privileges do administrador da SVM.

  Os Privileges do administrador de cluster são necessários para criar SVMs e LIFs. Os Privileges de administrador do SVM são suficientes para outras tarefas de configuração de SMB.

- Você deseja usar a CLI, não o System Manager ou uma ferramenta de script automatizado.

  Para usar o System Manager para configurar o acesso multiprotocolo nas, "Provisionar storage nas para Windows e Linux usando NFS e SMB"consulte .

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.

Detalhes sobre a sintaxe de comando estão disponíveis nas páginas de ajuda CLI e man do ONTAP.

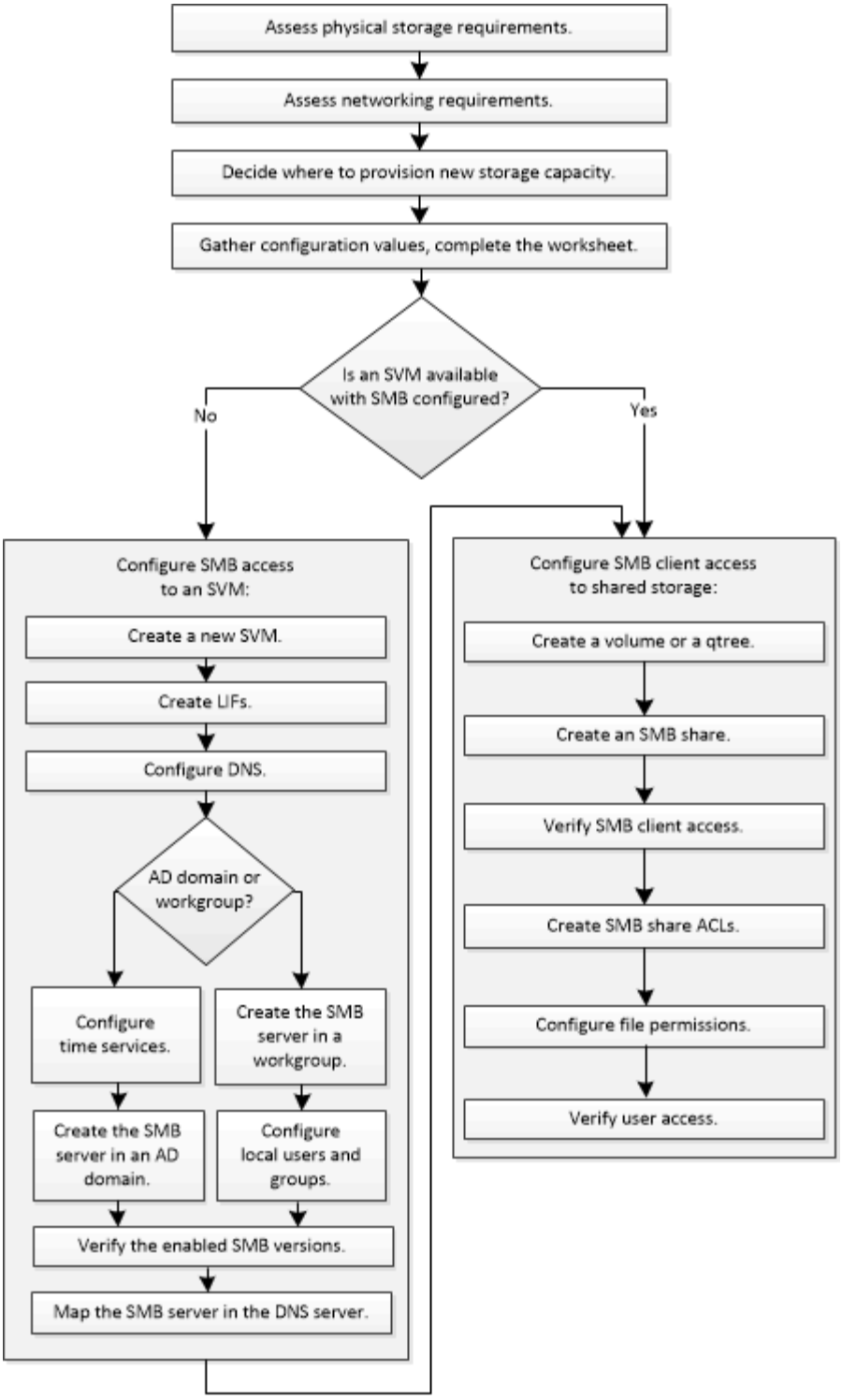
Se pretender obter detalhes sobre a gama de capacidades do protocolo SMB do ONTAP, consulte o "Visão geral de referência SMB".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Consulte…
O Gerenciador de sistema redesenhado (disponível com o ONTAP 9.7 e posterior)	"Provisione storage nas para servidores Windows usando SMB"
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da configuração SMB"

Fluxo de trabalho de configuração SMB

A configuração do SMB envolve a avaliação dos requisitos de storage físico e rede e, depois, a escolha de um fluxo de trabalho específico para sua meta; a configuração do acesso SMB a uma SVM nova ou existente ou a adição de um volume ou qtree a uma SVM existente que já esteja totalmente configurada para acesso SMB.



Preparação

Avaliar os requisitos de armazenamento físico

Antes de provisionar o storage SMB para clientes, você deve garantir que haja espaço suficiente em um agregado existente para o novo volume. Se não houver, você poderá adicionar discos a um agregado existente ou criar um novo agregado do tipo desejado.

Passos

1. Exibir espaço disponível em agregados existentes: `storage aggregate show`

   Se houver um agregado com espaço suficiente, Registre seu nome na Planilha.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Se não houver agregados com espaço suficiente, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede

Antes de fornecer armazenamento SMB aos clientes, você deve verificar se a rede está configurada corretamente para atender aos requisitos de provisionamento SMB.

Antes de começar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)
- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Passos

1. Exiba as portas físicas e virtuais disponíveis: `network port show`
   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.
   - Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o

melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis: `network subnet show`

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis: `network ipspace show`

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster: `network options ipv6 show`

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decida onde provisionar nova capacidade de storage SMB

Antes de criar um novo volume ou qtree SMB, você precisa decidir se deve colocá-lo em uma SVM nova ou existente e quanto de configuração o SVM precisa. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um volume ou qtree em um novo SVM ou em um SVM existente que tenha o SMB habilitado, mas não configurado, execute as etapas em ""Configurando o acesso SMB a um SVM"" e "adicionando capacidade de storage a um SVM habilitado para SMB".

  Configurando o acesso SMB a uma SVM

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

  Você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

  - Você está habilitando o SMB em um cluster pela primeira vez.
  - Você tem SVMs existentes em um cluster no qual não deseja ativar o suporte a SMB.
  - Você tem um ou mais SVMs habilitados para SMB em um cluster e deseja uma das seguintes conexões:
    - Para uma floresta ou grupo de trabalho diferente do ative Directory.
    - Para um servidor SMB em um namespace isolado (cenário de alocação a vários clientes). Você também deve escolher essa opção para provisionar storage em uma SVM existente que tenha SMB habilitado, mas não configurado. Esse pode ser o caso se você criou o SVM para acesso à SAN ou se nenhum protocolo foi habilitado quando o SVM foi criado.

  Depois de ativar o SMB no SVM, proceda ao provisionamento de um volume ou qtree.

- Se você quiser provisionar um volume ou qtree em um SVM existente totalmente configurado para acesso SMB, execute as etapas em ""adicionando capacidade de storage a um SVM habilitado para SMB"".

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

Folha de cálculo para recolher informações de configuração SMB

A folha de cálculo de configuração SMB permite-lhe recolher as informações necessárias para configurar o acesso SMB para clientes.

Você deve completar uma ou ambas as seções da Planilha, dependendo da decisão tomada sobre onde provisionar o armazenamento:

- Se você estiver configurando o acesso SMB a um SVM, deve concluir ambas as seções.

  Configurando o acesso SMB a uma SVM

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

- Se você estiver adicionando capacidade de storage a uma SVM habilitada para SMB, deverá concluir apenas a segunda seção.

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

As páginas de manual do comando contêm detalhes sobre os parâmetros.

Configurando o acesso SMB a uma SVM

Parâmetros para criar um SVM

Você fornece esses valores com o `vserver create` comando se estiver criando um novo SVM.

Campo	Descrição	O seu valor
`-vserver`	Nome fornecido para o novo SVM que é um nome de domínio totalmente qualificado (FQDN) ou que segue outra convenção que impõe nomes exclusivos de SVM em um cluster.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para a nova capacidade de armazenamento SMB.	
`-rootvolume`	Um nome exclusivo fornecido para o volume raiz da SVM.	
`-rootvolume-security-style`	Use o estilo de segurança NTFS para o SVM.	`ntfs`
`-language`	Use a configuração de idioma padrão neste fluxo de trabalho.	`C.UTF-8`

Campo	Descrição	O seu valor
`ipspace`	Opcional: Os IPspaces são espaços de endereço IP distintos nos quais os SVMs residem.	

Parâmetros para criar um LIF

Você fornece esses valores com o `network interface create` comando quando você está criando LIFs.

Campo	Descrição	O seu valor
`-lif`	Um nome que você fornece para o novo LIF.	
`-role`	Use a função de LIF de dados neste fluxo de trabalho.	`data`
`-data-protocol`	Utilize apenas o protocolo SMB neste fluxo de trabalho.	`cifs`
`-home-node`	O nó ao qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-home-port`	A porta ou grupo de interface para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-address`	O endereço IPv4 ou IPv6 no cluster que será usado para acesso aos dados pelo novo LIF.	
`-netmask`	A máscara de rede e o gateway para o LIF.	
`-subnet`	Um conjunto de endereços IP. Usado em vez `-address` de e `-netmask` para atribuir endereços e netmasks automaticamente.	
`-firewall-policy`	Use a política de firewall de dados padrão neste fluxo de trabalho.	`data`

Campo	Descrição	O seu valor
`-auto-revert`	Opcional: Especifica se um LIF de dados é automaticamente revertido para seu nó inicial na inicialização ou em outras circunstâncias. A predefinição é `false`.	

Parâmetros para resolução de nome de host DNS

Você fornece esses valores com o `vserver services name-service dns create` comando quando você está configurando o DNS.

Campo	Descrição	O seu valor
`-domains`	Até cinco nomes de domínio DNS.	
`-name-servers`	Até três endereços IP para cada servidor de nomes DNS.	

Configurando um servidor SMB em um domínio do ative Directory

Parâmetros para configuração do serviço de tempo

Você fornece esses valores com o `cluster time-service ntp server create` comando quando você está configurando serviços de tempo.

Campo	Descrição	O seu valor
`-server`	O nome do host ou o endereço IP do servidor NTP para o domínio do ative Directory.	

Parâmetros para criar um servidor SMB em um domínio do ative Directory

Você fornece esses valores com o `vserver cifs create` comando ao criar um novo servidor SMB e especificar informações de domínio.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o servidor SMB.	
`-cifs-server`	O nome do servidor SMB (até 15 carateres).	

Campo	Descrição	O seu valor
`-domain`	O nome de domínio totalmente qualificado (FQDN) do domínio do ative Directory a associar ao servidor SMB.	
`-ou`	Opcional: A unidade organizacional dentro do domínio do ative Directory a associar ao servidor SMB. Por padrão, este parâmetro é definido como computadores.	
`-netbios-aliases`	Opcional: Uma lista de aliases NetBIOS, que são nomes alternativos ao nome do servidor SMB.	
`-comment`	Opcional: Um comentário de texto para o servidor. Os clientes Windows podem ver esta descrição do servidor SMB ao navegar em servidores na rede.	

Configurando um servidor SMB em um grupo de trabalho

Parâmetros para criar um servidor SMB em um grupo de trabalho

Você fornece esses valores com o `vserver cifs create` comando ao criar um novo servidor SMB e especificar versões SMB compatíveis.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o servidor SMB.	
`-cifs-server`	O nome do servidor SMB (até 15 carateres).	
`-workgroup`	O nome do grupo de trabalho (até 15 carateres).	
`-comment`	Opcional: Um comentário de texto para o servidor. Os clientes Windows podem ver esta descrição do servidor SMB ao navegar em servidores na rede.	

Parâmetros para criar usuários locais

Você fornece esses valores ao criar usuários locais usando o `vserver cifs users-and-groups local-user create` comando. Eles são necessários para servidores SMB em grupos de trabalho e opcionais em domínios do AD.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o usuário local.	
`-user-name`	O nome do utilizador local (até 20 carateres).	
`-full-name`	Opcional: O nome completo do usuário. Se o nome completo contiver um espaço, insira o nome completo entre aspas duplas.	
`-description`	Opcional: Uma descrição para o usuário local. Se a descrição contiver um espaço, coloque o parâmetro entre aspas.	
`-is-account-disabled`	Opcional: Especifica se a conta de usuário está ativada ou desativada. Se este parâmetro não for especificado, o padrão é ativar a conta de usuário.	

Parâmetros para criar grupos locais

Você fornece esses valores ao criar grupos locais usando o `vserver cifs users-and-groups local-group create` comando. Eles são opcionais para servidores SMB em domínios e grupos de trabalho do AD.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o grupo local.	
`-group-name`	O nome do grupo local (até 256 carateres).	
`-description`	Opcional: Uma descrição para o grupo local. Se a descrição contiver um espaço, coloque o parâmetro entre aspas.	

Adição de capacidade de storage a uma SVM habilitada para SMB

Parâmetros para criar um volume

Você fornece esses valores com o `volume create` comando se estiver criando um volume em vez de uma qtree.

Campo	Descrição	O seu valor
`-vserver`	Nome de uma SVM nova ou existente que hospedará o novo volume.	
`-volume`	Um nome descritivo exclusivo que você fornece para o novo volume.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para o novo volume SMB.	
`-size`	Um número inteiro fornecido para o tamanho do novo volume.	
`-security-style`	Utilize o estilo de segurança NTFS para este fluxo de trabalho.	`ntfs`
`-junction-path`	Localização sob a raiz (/) onde o novo volume deve ser montado.	

Parâmetros para criar uma qtree

Você fornece esses valores com o `volume qtree create` comando se estiver criando uma qtree em vez de um volume.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual reside o volume que contém a qtree.	
`-volume`	O nome do volume que conterá a nova qtree.	
`-qtree`	Um nome descritivo exclusivo que você fornece para a nova qtree, 64 carateres ou menos.	
`-qtree-path`	O argumento de caminho de qtree no formato `/vol/volume_name/qtree_name\>` pode ser especificado em vez de especificar volume e qtree como argumentos separados.	

Parâmetros para criar compartilhamentos SMB

Você fornece esses valores com o `vserver cifs share create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o compartilhamento SMB.	
`-share-name`	O nome do compartilhamento SMB que você deseja criar (até 256 carateres).	
`-path`	O nome do caminho para o compartilhamento SMB (até 256 carateres). Esse caminho deve existir em um volume antes de criar o compartilhamento.	
`-share-properties`	Opcional: Uma lista de propriedades de compartilhamento. As predefinições são `oplocks`, `browsable`, `changenotify` e `show-previous-versions`.	
`-comment`	Opcional: Um comentário de texto para o servidor (até 256 carateres). Os clientes Windows podem ver esta descrição do compartilhamento SMB ao navegar na rede.	

Parâmetros para criar listas de controle de acesso (ACLs) de compartilhamento SMB

Você fornece esses valores com o `vserver cifs share access-control create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome da SVM no qual criar a ACL SMB.	
`-share`	O nome do compartilhamento SMB no qual criar.	
`-user-group-type`	O tipo de usuário ou grupo a ser adicionado à ACL do compartilhamento. O tipo padrão é `windows`	`windows`

Campo	Descrição	O seu valor
`-user-or-group`	O usuário ou grupo a adicionar à ACL do compartilhamento. Se você especificar o nome de usuário, você deve incluir o domínio do usuário usando o formato "nome de usuário".	
`-permission`	Especifica as permissões para o usuário ou grupo.	`[No_access
Read	Change	Full_Control]`

Configurar o acesso SMB a uma SVM

Configurar o acesso SMB a uma SVM

Se você ainda não tiver um SVM configurado para acesso de cliente SMB, crie e configure um novo SVM ou configure um SVM existente. A configuração do SMB envolve a abertura do acesso ao volume raiz do SVM, a criação de um servidor SMB, a criação de um LIF, a ativação da resolução do nome de host, a configuração de serviços de nome e, se desejado, a ativação da segurança Kerberos.

Criar um SVM

Se você ainda não tiver pelo menos um SVM em um cluster para fornecer acesso aos dados a clientes SMB, será necessário criar um.

Antes de começar

- A partir do ONTAP 9.13,1, é possível definir uma capacidade máxima para uma VM de armazenamento. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

Passos

1. Criar um SVM: `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - Utilize a definição NTFS para a `-rootvolume-security-style` opção.
   - Utilize a opção C.UTF-8 predefinida `-language`.
   - A `ipspace` definição é opcional.
2. Verifique a configuração e o status do SVM recém-criado: `vserver show -vserver` *`vserver_name`*

   O `Allowed Protocols` campo deve incluir CIFS. Você pode editar esta lista mais tarde.

   O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no IPspace : `ipspaceA`

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
                Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                       Vserver Admin State: running
                 Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

A partir do ONTAP 9.13,1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Verifique se o protocolo SMB está ativado na SVM

Antes de poder configurar e utilizar SMB em SVMs, tem de verificar se o protocolo está ativado.

Sobre esta tarefa

Isso geralmente é feito durante a configuração do SVM, mas se você não ativou o protocolo durante a configuração, poderá ativá-lo mais tarde usando o `vserver add-protocols` comando.

Não é possível adicionar ou remover um protocolo de um LIF depois de criado.

Você também pode desativar protocolos em SVMs usando o `vserver remove-protocols` comando.

Passos

1. Verifique quais protocolos estão atualmente ativados e desativados para o SVM: `vserver show -vserver vserver_name -protocols`

   Você também pode usar o `vserver show-protocols` comando para exibir os protocolos atualmente habilitados em todos os SVMs no cluster.

2. Se necessário, ative ou desative um protocolo:
   - Para ativar o protocolo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Para desativar um protocolo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirme se os protocolos ativados e desativados foram atualizados corretamente: `vserver show -vserver vserver_name -protocols`

Exemplo

O comando a seguir exibe quais protocolos estão atualmente ativados e desativados (permitidos e não permitidos) no SVM chamado VS1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

O comando a seguir permite o acesso por SMB adicionando `cifs` à lista de protocolos habilitados no SVM chamado VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Abra a política de exportação do volume raiz da SVM

A política de exportação padrão do volume raiz da SVM deve incluir uma regra para permitir que todos os clientes tenham acesso aberto por meio do SMB. Sem essa regra,

todos os clientes SMB têm acesso negado ao SVM e seus volumes.

Sobre esta tarefa

Quando um novo SVM é criado, uma política de exportação padrão (chamada padrão) é criada automaticamente para o volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM.

Você deve verificar se todo o acesso SMB está aberto na política de exportação padrão e, mais tarde, restringir o acesso a volumes individuais criando políticas de exportação personalizadas para volumes individuais ou qtrees.

Passos

1. Se você estiver usando uma SVM existente, verifique a política de exportação de volume raiz padrão: `vserver export-policy rule show`

   A saída do comando deve ser semelhante ao seguinte:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol: cifs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                               RO Access Rule: any
                               RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   Se existir uma regra que permita o acesso aberto, esta tarefa está concluída. Caso contrário, avance para o passo seguinte.

2. Crie uma regra de exportação para o volume raiz da SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verifique a criação de regras usando o `vserver export-policy rule show` comando.

Resultados

Qualquer cliente SMB agora pode acessar qualquer volume ou qtree criado no SVM.

Crie um LIF

Um LIF é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

Passos

1. Criar um LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

ONTAP 9 .5 e anteriores
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9 1.6 e posterior
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - O `-role` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6).
   - O `-data-protocol` parâmetro não é necessário ao criar um LIF usando uma política de serviço

(começando com ONTAP 9.6). Ao usar o ONTAP 9.5 e anteriores, o `-data-protocol` parâmetro deve ser especificado quando o LIF é criado e não pode ser modificado mais tarde sem destruir e recriar o LIF de dados.

- `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

  Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.

2. Verifique se o LIF foi criado com sucesso:

   ```
   network interface show
   ```

3. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

O comando a seguir mostra como criar um LIF de dados nas atribuído com a `default-data-files` política de serviço:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Ative DNS para resolução de nome de host

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os

nomes de host são resolvidos usando servidores DNS externos.

Antes de começar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

O *Network Management Guide* contém informações sobre a configuração de DNS dinâmico na SVM.

Passos

1. Habilite o DNS na SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   A partir do ONTAP 9.2, o `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Exiba as configurações do domínio DNS usando o `vserver services name-service dns show` comando. ""

   O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

   ```
   vserver services name-service dns show
                                              Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide o status dos servidores de nomes usando o `vserver services name-service dns check` comando.

   O `vserver services name-service dns check` comando está disponível a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configure um servidor SMB em um domínio do ative Directory

Configurar serviços de tempo

Antes de criar um servidor SMB em um controlador de domínio ativo, você deve garantir que a hora do cluster e a hora nos controladores de domínio do domínio ao qual o servidor SMB pertencerá correspondem dentro de cinco minutos.

Sobre esta tarefa

Você deve configurar os serviços NTP do cluster para usar os mesmos servidores NTP para sincronização de tempo que o domínio do ative Directory usa.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Passos

1. Configure os serviços de tempo usando o `cluster time-service ntp server create` comando.
   - Para configurar serviços de tempo sem autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address`
   - Para configurar serviços de tempo com autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Verifique se os serviços de tempo estão configurados corretamente usando o `cluster time-service ntp server show` comando.

```
cluster time-service ntp server show
```

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Comandos para gerenciar a autenticação simétrica em servidores NTP

A partir do ONTAP 9.5, o protocolo de tempo de rede (NTP) versão 3 é suportado. O NTPv3 inclui autenticação simétrica usando chaves SHA-1, o que aumenta a segurança da rede.

Para fazer isso…	Use este comando…
Configurar um servidor NTP sem autenticação simétrica	`cluster time-service ntp server create -server server_name`
Configure um servidor NTP com autenticação simétrica	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Ativar autenticação simétrica para um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID de chave necessária.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configurar uma chave NTP partilhada	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` As chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP
Configure um servidor NTP com um ID de chave desconhecido	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure um servidor com um ID de chave não configurado no servidor NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` O ID, tipo e valor da chave devem ser idênticos ao ID, tipo e valor da chave configurados no servidor NTP.

Para fazer isso…	Use este comando…
Desativar a autenticação simétrica	`cluster time-service ntp server modify -server server_name -authentication disabled`

Crie um servidor SMB em um domínio do ative Directory

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o domínio do ative Directory (AD) ao qual ele pertence.

Antes de começar

Os SVM e LIFs que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB. Os LIFs devem ser capazes de se conetar aos servidores DNS configurados no SVM e a um controlador de domínio AD do domínio ao qual você deseja ingressar no servidor SMB.

Qualquer usuário autorizado a criar contas de máquina no domínio do AD ao qual você está ingressando no servidor SMB pode criar o servidor SMB no SVM. Isso pode incluir usuários de outros domínios.

A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

Sobre esta tarefa

Ao criar um servidor SMB em um domínio do diretório de atividades:

- Você deve usar o nome de domínio totalmente qualificado (FQDN) ao especificar o domínio.
- A configuração padrão é adicionar a conta de máquina do servidor SMB ao objeto de computador do ative Directory.
- Pode optar por adicionar o servidor SMB a uma unidade organizacional (ou) diferente utilizando a `-ou` opção.
- Opcionalmente, você pode optar por adicionar uma lista delimitada por vírgulas de um ou mais aliases NetBIOS (até 200) para o servidor SMB.

  A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores originais.

As `vserver cifs` páginas man contêm parâmetros opcionais adicionais e requisitos de nomeação.

> A partir do ONTAP 9.1, você pode habilitar o SMB versão 2,0 para se conetar a um controlador de domínio (DC). Isso é necessário se você desativou o SMB 1,0 em controladores de domínio. A partir do ONTAP 9.2, o SMB 2,0 é ativado por padrão.

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas. O ONTAP requer criptografia para comunicações do controlador de domínio quando a `-encryption-required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3. .

"Gerenciamento de SMB" Contém mais informações sobre as opções de configuração do servidor SMB.

Passos

1. Verifique se o SMB está licenciado no cluster: `system license show -package cifs`

   A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

   Não é necessária uma licença CIFS se o servidor SMB for utilizado apenas para autenticação.

2. Crie o servidor SMB em um domínio AD: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

   O comando a seguir cria o servidor SMB "sssmb_server01" no domínio "'example.com`":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   O comando a seguir cria o servidor SMB "sssmb_server02" no domínio "mydomain.com`" e autentica o administrador do ONTAP com um arquivo keytab:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

   Neste exemplo, o comando output mostra que um servidor SMB chamado "'SMB_SERVER01'" foi criado na SVM vs1.example.com e foi associado ao domínio "'example.com`".

   ```
   cluster1::> vserver cifs show -vserver vs1

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                              Authentication Style: domain
                 CIFS Server Administrative Status: up
                           CIFS Server Description: -
                           List of NetBIOS Aliases: -
   ```

4. Se desejar, ative a comunicação criptografada com o controlador de domínio (ONTAP 9.8 e posterior): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc -connection true`

Exemplos

O comando a seguir cria um servidor SMB chamado "ssssmb_server02" no SVM vs2.example.com no domínio "'example.com`". A conta da máquina é criada no contentor "'ou-eng, ou-corp, DC-example, DC-com'". Ao servidor SMB é atribuído um alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

O comando a seguir permite que um usuário de um domínio diferente, neste caso um administrador de um domínio confiável, crie um servidor SMB chamado "sssmb_server03" no SVM vs3.example.com. A `-domain` opção especifica o nome do domínio inicial (especificado na configuração DNS) no qual você deseja criar o servidor SMB. A `username` opção especifica o administrador do domínio confiável.

- Domínio doméstico: example.com
- Domínio confiável: trust.lab.com
- Nome de usuário para o domínio confiável: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Crie arquivos keytab para autenticação SMB

A partir do ONTAP 9.7, o ONTAP oferece suporte à autenticação SVM com servidores do ative Directory (AD) usando arquivos keytab. Os ADMINISTRADORES DE ANÚNCIOS geram um arquivo keytab e o disponibilizam aos administradores do ONTAP como um URI (identificador de recurso uniforme), que é fornecido quando `vserver cifs` os

comandos exigem autenticação Kerberos com o domínio AD.

Os ADMINISTRADORES DE ANÚNCIOS podem criar os arquivos keytab usando o comando padrão do Windows Server `ktpass`. O comando deve ser executado no domínio primário onde a autenticação é necessária. O `ktpass` comando pode ser usado para gerar arquivos keytab somente para usuários de domínio primário; chaves geradas usando usuários de domínio confiável não são suportadas.

Os arquivos keytab são gerados para usuários administrativos específicos do ONTAP. Desde que a senha do usuário administrativo não seja alterada, as chaves geradas para o tipo de criptografia e domínio específicos não serão alteradas. Portanto, um novo arquivo keytab é necessário sempre que a senha do usuário admin é alterada.

São suportados os seguintes tipos de encriptação:

- AES256-SHA1
- DES-CBC-MD5

> O ONTAP não oferece suporte ao tipo de criptografia DES-CBC-CRC.

- RC4-HMAC

AES256 é o tipo de criptografia mais alto e deve ser usado se ativado no sistema ONTAP.

Os arquivos keytab podem ser gerados especificando a senha de administrador ou usando uma senha gerada aleatoriamente. No entanto, a qualquer momento, apenas uma opção de senha pode ser usada, porque uma chave privada específica para o usuário admin é necessária no servidor AD para descriptografar as chaves dentro do arquivo keytab. Qualquer alteração na chave privada para um administrador específico invalidará o arquivo keytab.

Configure um servidor SMB em um grupo de trabalho

Configure um servidor SMB em uma visão geral do grupo de trabalho

A configuração de um servidor SMB como membro em um grupo de trabalho consiste em criar o servidor SMB e, em seguida, criar usuários e grupos locais.

Você pode configurar um servidor SMB em um grupo de trabalho quando a infraestrutura de domínio do Microsoft ative Directory não estiver disponível.

Um servidor SMB no modo de grupo de trabalho suporta apenas autenticação NTLM e não suporta autenticação Kerberos.

Crie um servidor SMB em um grupo de trabalho

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o grupo de trabalho ao qual ele pertence.

Antes de começar

Os SVM e LIFs que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB. Os LIFs devem ser capazes de se conetar aos servidores DNS configurados no SVM.

Sobre esta tarefa

Os servidores SMB no modo de grupo de trabalho não suportam os seguintes recursos SMB:

- Protocolo de SMB3 testemunhas
- SMB3 ações da CA
- SQL sobre SMB
- Redirecionamento de pasta
- Perfis de roaming
- Objeto de política de grupo (GPO)
- Serviço de Snapshot de volume (VSS)

As `vserver cifs` páginas man contêm parâmetros de configuração opcionais adicionais e requisitos de nomenclatura.

Passos

1. Verifique se o SMB está licenciado no cluster: `system license show -package cifs`

   A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

   Não é necessária uma licença CIFS se o servidor SMB for utilizado apenas para autenticação.

2. Crie o servidor SMB em um grupo de trabalho: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   O comando a seguir cria o servidor SMB "ssssmb_server01" no grupo de trabalho "'workgroup01":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

   No exemplo a seguir, o comando output mostra que um servidor SMB chamado "sssmb_server01" foi criado na SVM vs1.example.com no grupo de trabalho "'workgroup01"":

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

Depois de terminar

Para um servidor CIFS em um grupo de trabalho, você deve criar usuários locais e, opcionalmente, grupos locais, no SVM.

Informações relacionadas

"Gerenciamento de SMB"

Crie contas de usuário locais

Você pode criar uma conta de usuário local que pode ser usada para autorizar o acesso aos dados contidos no SVM em uma conexão SMB. Você também pode usar contas de usuário locais para autenticação ao criar uma sessão SMB.

Sobre esta tarefa

A funcionalidade de usuário local é ativada por padrão quando o SVM é criado.

Ao criar uma conta de usuário local, você deve especificar um nome de usuário e especificar o SVM para associar a conta.

As `vserver cifs users-and-groups local-user` páginas man contêm detalhes sobre parâmetros opcionais e requisitos de nomeação.

Passos

1. Crie o usuário local: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Os seguintes parâmetros opcionais podem ser úteis:

   - `-full-name`

     O nome completo dos usuários.

   - `-description`

     Uma descrição para o utilizador local.

   - `-is-account-disabled {true|false}`

     Especifica se a conta de usuário está ativada ou desativada. Se este parâmetro não for especificado, o padrão é ativar a conta de usuário.

   O comando solicita a senha do usuário local.

2. Introduza uma palavra-passe para o utilizador local e, em seguida, confirme a palavra-passe.
3. Verifique se o usuário foi criado com sucesso: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir cria um usuário local ""SMB_SERVER01"", com um nome completo ""Sue Chang"", associado ao SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator            Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Crie grupos locais

É possível criar grupos locais que podem ser usados para autorizar o acesso aos dados associados ao SVM em uma conexão SMB. Você também pode atribuir Privileges que definem quais direitos de usuário ou recursos um membro do grupo tem.

Sobre esta tarefa

A funcionalidade de grupo local é ativada por padrão quando o SVM é criado.

Ao criar um grupo local, você deve especificar um nome para o grupo e especificar o SVM para associar o grupo. Você pode especificar um nome de grupo com ou sem o nome de domínio local e, opcionalmente, especificar uma descrição para o grupo local. Não é possível adicionar um grupo local a outro grupo local.

As `vserver cifs users-and-groups local-group` páginas man contêm detalhes sobre parâmetros opcionais e requisitos de nomeação.

Passos

1. Crie o grupo local: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   O seguinte parâmetro opcional pode ser útil:

   - `-description`

     Uma descrição para o grupo local.

2. Verifique se o grupo foi criado com sucesso: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemplo

O exemplo a seguir cria um grupo local "SMB_SERVER01" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Depois de terminar

Você deve adicionar membros ao novo grupo.

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Se você não quiser mais que um usuário local, usuário de domínio ou grupo de domínio tenha direitos de acesso ou Privileges com base na associação a um grupo, você pode remover o membro do grupo.

Você deve ter em mente o seguinte ao adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o ONTAP deve ser capaz de resolver o nome para um SID.

Você deve ter em mente o seguinte ao remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- Para remover um membro de um grupo local, o ONTAP deve ser capaz de resolver seu nome para um SID.

Passos

1. Adicione um membro ou remova um membro de um grupo.
   - Adicionar um membro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.

- Remover um membro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.

Exemplos

O exemplo a seguir adiciona um usuário local ""SMB_SERVER01"" ao grupo local ""SMB_SERVER01" engenharia" no SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

O exemplo a seguir remove os usuários locais "'SMB_SERVER01"" e "'SMB_SERVER01' james' do grupo local "'SMB_SERVER01' Engineering" no SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verifique as versões do SMB ativadas

Sua versão do ONTAP 9 determina quais versões do SMB estão habilitadas por padrão para conexões com clientes e controladores de domínio. Você deve verificar se o servidor SMB oferece suporte aos clientes e às funcionalidades necessárias em seu ambiente.

Sobre esta tarefa

Para conexões com clientes e controladores de domínio, você deve ativar o SMB 2,0 e posterior sempre que possível. Por motivos de segurança, você deve evitar o uso do SMB 1,0 e desativá-lo se tiver verificado que não é necessário no seu ambiente.

No ONTAP 9, as versões 2,0 e posteriores do SMB são ativadas por padrão para conexões de clientes, mas a versão do SMB 1,0 habilitada por padrão depende da versão do ONTAP.

- A partir do ONTAP 9 P8.1, o SMB 1,0 pode ser desativado em SVMs.

  A `-smb1-enabled` opção para o `vserver cifs options modify` comando ativa ou desativa o SMB 1,0.

- Começando com ONTAP 9.3, ele é desativado por padrão em novos SVMs.

Se o servidor SMB estiver em um domínio do ative Directory (AD), você poderá habilitar o SMB 2,0 para se conetar a um controlador de domínio (DC) começando com o ONTAP 9.1. Isso é necessário se você tiver desabilitado o SMB 1,0 em DCs. A partir do ONTAP 9.2, o SMB 2,0 é ativado por padrão para conexões DC.

Se `-smb1-enabled-for-dc-connections` estiver definido como `false` enquanto `-smb1-enabled` estiver definido como `true`, o ONTAP nega conexões SMB 1,0 como cliente, mas continua a aceitar conexões SMB 1,0 de entrada como servidor.

"Gerenciamento de SMB" Contém detalhes sobre as versões e funcionalidades do SMB suportadas.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Verifique quais versões SMB estão ativadas:

```
vserver cifs options show
```

Você pode rolar a lista para baixo para exibir as versões SMB habilitadas para conexões de cliente e, se estiver configurando um servidor SMB em um domínio AD, para conexões de domínio AD.

3. Ative ou desative o protocolo SMB para ligações de clientes, conforme necessário:
   - Para ativar uma versão SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

Valores possíveis para `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

O comando a seguir habilita o SMB 3,1 no SVM vs1.example.com:
`cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

   - Para desativar uma versão SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Se o servidor SMB estiver em um domínio do ative Directory, ative ou desative o protocolo SMB para conexões DC, conforme necessário:
   - Para ativar uma versão SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

- Para desativar uma versão SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Mapeie o servidor SMB no servidor DNS

O servidor DNS do seu site deve ter uma entrada apontando o nome do servidor SMB e quaisquer aliases NetBIOS para o endereço IP do LIF de dados para que os usuários do Windows possam mapear uma unidade para o nome do servidor SMB.

Antes de começar

Você deve ter acesso administrativo ao servidor DNS do seu site. Se não tiver acesso administrativo, deverá pedir ao administrador DNS para executar esta tarefa.

Sobre esta tarefa

Se você usar aliases NetBIOS para o nome do servidor SMB, é uma prática recomendada criar pontos de entrada de servidor DNS para cada alias.

Passos

1. Inicie sessão no servidor DNS.
2. Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP do LIF de dados.
3. Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico Alias (CNAME resource record) para mapear cada alias para o endereço IP do LIF de dados do servidor SMB.

Resultados

Depois que o mapeamento é propagado pela rede, os usuários do Windows podem mapear uma unidade para o nome do servidor SMB ou seus aliases NetBIOS.

Configurar o acesso de cliente SMB ao armazenamento partilhado

Configurar o acesso de cliente SMB ao armazenamento partilhado

Para fornecer acesso de cliente SMB ao storage compartilhado em uma SVM, você precisa criar um volume ou qtree para fornecer um contêiner de storage e, em seguida, criar ou modificar um compartilhamento para esse contêiner. Em seguida, você pode configurar permissões de compartilhamento e arquivo e testar o acesso a partir de

sistemas cliente.

Antes de começar

- O SMB deve estar completamente configurado no SVM.
- Todas as atualizações da configuração dos serviços de nome devem estar concluídas.
- Quaisquer adições ou modificações a um domínio do ative Directory ou configuração de grupo de trabalho devem estar concluídas.

Crie um volume ou um contêiner de storage de qtree

Crie um volume

Você pode criar um volume e especificar seu ponto de junção e outras propriedades usando o `volume create` comando.

Sobre esta tarefa

Um volume deve incluir um *caminho de junção* para que seus dados sejam disponibilizados aos clientes. Você pode especificar o caminho de junção ao criar um novo volume. Se você criar um volume sem especificar um caminho de junção, será necessário *montar* o volume no namespace SVM usando o `volume mount` comando.

Antes de começar

- O SMB deve ser configurado e executado.
- O estilo de segurança da SVM deve ser NTFS.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*`]`

   As opções para `-junction-path` são as seguintes:

   - Diretamente sob a raiz, por exemplo, `/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado diretamente no volume raiz da SVM.

   - Em um diretório existente, por exemplo, `/existing_dir/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado em um volume existente (em uma hierarquia existente), expresso como um diretório.

   Se você quiser criar um volume em um novo diretório (em uma nova hierarquia em um novo volume), por exemplo, `/new_dir/new_vol` será necessário criar primeiro um novo volume pai que seja juntado ao

volume raiz SVM. Em seguida, você criaria o novo volume filho no caminho de junção do novo volume pai (novo diretório).

2. Verifique se o volume foi criado com o ponto de junção desejado: `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Exemplos

O comando a seguir cria um novo volume chamado users1 no SVM vs1.example.com e no agregado aggr1. O novo volume é disponibilizado em `/users`. O volume tem 750 GB de tamanho e sua garantia de volume é do tipo volume (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

O comando a seguir cria um novo volume chamado "'home4" na SVM"'vs1.example.com`'" e o agregado "'aggr1". O diretório `/eng/` já existe no namespace para o VS1 SVM, e o novo volume é disponibilizado no `/eng/home`, que se torna o diretório home do `/eng/` namespace. O volume é de 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Crie uma qtree

Você pode criar uma qtree para conter seus dados e especificar suas propriedades usando o `volume qtree create` comando.

Antes de começar

- O SVM e o volume que conterá a nova qtree já devem existir.
- O estilo de segurança da SVM deve ser NTFS e o SMB deve ser configurado e executado.

Passos

1. Crie a qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Você pode especificar o volume e a qtree como argumentos separados ou especificar o argumento de caminho de qtree no formato `/vol/volume_name/_qtree_name`.

2. Verifique se a qtree foi criada com o caminho de junção desejado: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Exemplo

O exemplo a seguir cria uma qtree chamada qt01 localizada no SVM vs1.example.com que tem um caminho de junção `/vol/data1` :

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Requisitos e considerações para criar um compartilhamento SMB

Antes de criar um compartilhamento SMB, você deve entender os requisitos para caminhos de compartilhamento e propriedades de compartilhamento, especialmente para diretórios base.

Criar um compartilhamento SMB implica especificar uma estrutura de caminho de diretório (usando a `-path` opção no `vserver cifs share create` comando) que os clientes acessarão. O caminho do diretório corresponde ao caminho de junção de um volume ou qtree que você criou no namespace SVM. O caminho do diretório e o caminho de junção correspondente devem existir antes de criar seu compartilhamento.

Os caminhos de compartilhamento têm os seguintes requisitos:

- Um nome de caminho de diretório pode ter até 255 carateres.
- Se houver um espaço no nome do caminho, toda a cadeia de carateres deve ser colocada em aspas (por

exemplo, "`/new volume/mount here`").

- Se o caminho UNC (`\\servername\sharename\filepath`) do compartilhamento contiver mais de 256 carateres (excluindo o "\" inicial no caminho UNC), a guia **Segurança** na caixa Propriedades do Windows não estará disponível.

  Este é um problema de cliente do Windows em vez de um problema de ONTAP. Para evitar esse problema, não crie compartilhamentos com caminhos UNC com mais de 256 carateres.

Os padrões de propriedade de compartilhamento podem ser alterados:

- As propriedades iniciais padrão para todos os compartilhamentos são `oplocks`, `browsable`, `changenotify` e `show-previous-versions`.
- É opcional especificar propriedades de compartilhamento quando você cria um compartilhamento.

  No entanto, se você especificar propriedades de compartilhamento ao criar o compartilhamento, os padrões não serão usados. Se você usar o `-share-properties` parâmetro ao criar um compartilhamento, especifique todas as propriedades de compartilhamento que deseja aplicar ao compartilhamento usando uma lista delimitada por vírgulas.

- Para designar um compartilhamento de diretório base, use a `homedirectory` propriedade.

  Este recurso permite configurar um compartilhamento que mapeia para diferentes diretórios com base no usuário que se coneta a ele e um conjunto de variáveis. Em vez de ter que criar compartilhamentos separados para cada usuário, você pode configurar um único compartilhamento com alguns parâmetros do diretório base para definir a relação de um usuário entre um ponto de entrada (o compartilhamento) e seu diretório inicial (um diretório no SVM).

  ⓘ Não é possível adicionar ou remover esta propriedade depois de criar a partilha.

Os compartilhamentos do diretório base têm os seguintes requisitos:

- Antes de criar diretórios home do SMB, você deve adicionar pelo menos um caminho de pesquisa do diretório home usando o `vserver cifs home-directory search-path add` comando.
- Os compartilhamentos do diretório base especificados pelo valor de `homedirectory` no `-share -properties` parâmetro devem incluir a `%w` variável dinâmica (nome de usuário do Windows) no nome do compartilhamento.

  O nome do compartilhamento pode também conter a `%d` variável dinâmica (nome de domínio) (por exemplo, `%d/%w`) ou uma parte estática no nome do compartilhamento (por exemplo, `home1_%w`).

- Se o compartilhamento for usado por administradores ou usuários para se conetar a diretórios home de outros usuários (usando opções para o `vserver cifs home-directory modify` comando), o padrão de nome de compartilhamento dinâmico deve ser precedido por um til (~).

"Gerenciamento de SMB" e `vserver cifs share` as páginas de manual têm informações adicionais.

Crie um compartilhamento SMB

Você deve criar um compartilhamento SMB antes de compartilhar dados de um servidor SMB com clientes SMB. Ao criar um compartilhamento, você pode definir propriedades

de compartilhamento, como designar o compartilhamento como um diretório inicial. Você também pode personalizar o compartilhamento configurando configurações opcionais.

Antes de começar

O caminho do diretório para o volume ou qtree deve existir no namespace SVM antes de criar o compartilhamento.

Sobre esta tarefa

Quando você cria um compartilhamento, a ACL de compartilhamento padrão (permissões de compartilhamento padrão) é `Everyone / Full Control`. Depois de testar o acesso ao compartilhamento, você deve remover a ACL de compartilhamento padrão e substituí-la por uma alternativa mais segura.

Passos

1. Se necessário, crie a estrutura do caminho do diretório para o compartilhamento.

   O `vserver cifs share create` comando verifica o caminho especificado na `-path` opção durante a criação de compartilhamento. Se o caminho especificado não existir, o comando falhará.

2. Crie um compartilhamento SMB associado ao SVM especificado: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verifique se o compartilhamento foi criado:`vserver cifs share show -share-name share_name`

Exemplos

O comando a seguir cria um compartilhamento SMB chamado "'SHARE1" no SVM `vs1.example.com`. Seu caminho de diretório é `/users`, e é criado com propriedades padrão.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Verifique o acesso do cliente SMB

Você deve verificar se configurou o SMB corretamente acessando e gravando dados no compartilhamento. Você deve testar o acesso usando o nome do servidor SMB e quaisquer aliases NetBIOS.

Passos

1. Faça login em um cliente Windows.
2. Teste o acesso usando o nome do servidor SMB:

   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\SMB_Server_Name\Share_Name`

      Se o mapeamento não for bem-sucedido, é possível que o mapeamento DNS ainda não tenha se propagado pela rede. Você deve testar o acesso usando o nome do servidor SMB posteriormente.

      Se o servidor SMB tiver o nome vs1.example.com e o compartilhamento tiver o nome SHARE1, você deverá inserir o seguinte: `\\vs0.example.com\SHARE1`

   b. Na unidade recém-criada, crie um arquivo de teste e exclua o arquivo.

   Você verificou o acesso de gravação ao compartilhamento usando o nome do servidor SMB.

3. Repita a Etapa 2 para qualquer alias NetBIOS.

Criar listas de controle de acesso de compartilhamento SMB

A configuração de permissões de compartilhamento criando listas de controle de acesso (ACLs) para compartilhamentos SMB permite controlar o nível de acesso a um compartilhamento para usuários e grupos.

Antes de começar

Você deve ter decidido quais usuários ou grupos terão acesso ao compartilhamento.

Sobre esta tarefa

Você pode configurar ACLs de nível de compartilhamento usando nomes de usuário ou grupo do Windows locais ou de domínio.

Antes de criar uma nova ACL, você deve excluir a ACL de compartilhamento padrão `Everyone / Full Control` , que representa um risco de segurança.

No modo de grupo de trabalho, o nome de domínio local é o nome do servidor SMB.

Passos

1. Excluir a ACL de compartilhamento padrão:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure a nova ACL:

Se você quiser configurar ACLs usando um…	Digite o comando…
Usuário do Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`

Se você quiser configurar ACLs usando um…	Digite o comando…
Grupo Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. Verifique se a ACL aplicada ao compartilhamento está correta usando o `vserver cifs share access-control show` comando.

Exemplo

O comando a seguir `Change` dá permissões ao grupo Windows "equipe de vendas" para o compartilhamento "vendas" no vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

Os comandos a seguir `Change` dão permissão ao grupo local do Windows chamado "Tiger Team" e `Full_Control` permissão ao usuário local do Windows chamado "Sue Chang" para o compartilhamento "d.atavol5" no "VS1" SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configurar permissões de arquivo NTFS em um compartilhamento

Para habilitar o acesso a arquivos aos usuários ou grupos que têm acesso a um compartilhamento, você deve configurar permissões de arquivo NTFS em arquivos e diretórios nesse compartilhamento a partir de um cliente Windows.

Antes de começar

O administrador que executa esta tarefa deve ter permissões NTFS suficientes para alterar permissões nos objetos selecionados.

Sobre esta tarefa

"Gerenciamento de SMB" E a documentação do Windows contém informações sobre como definir permissões NTFS padrão e avançadas.

Passos

1. Inicie sessão num cliente Windows como administrador.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:

    a. Selecione uma letra **Drive**.

    b. Na caixa **pasta**, digite o nome do servidor SMB que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

    Se o nome do servidor SMB for SMB_SERVER01 e o compartilhamento for chamado "'SHARE1", você digitaria `\\SMB_SERVER01\SHARE1`.

Você pode especificar o endereço IP da interface de dados para o servidor SMB em vez do nome do servidor SMB.

c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

4. Selecione o arquivo ou diretório para o qual você deseja definir permissões de arquivo NTFS.
5. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
6. Selecione a guia **Segurança**.

   A guia Segurança exibe a lista de usuários e grupos para os quais a permissão NTFS está definida. A caixa permissões para <Object> exibe uma lista de permissões de permissão e negação em vigor para o usuário ou grupo selecionado.

7. Clique em **Editar**.

   A caixa permissões para <Object> será aberta.

8. Execute as ações desejadas:

Se você quiser	Faça o seguinte…
Defina permissões NTFS padrão para um novo usuário ou grupo	a. Clique em **Add**. A janela Selecionar usuário, computadores, contas de serviço ou grupos será exibida. b. Na caixa **Digite os nomes de objeto a selecionar**, digite o nome do usuário ou grupo no qual você deseja adicionar permissão NTFS. c. Clique em **OK**.
Alterar ou remover permissões NTFS padrão de um usuário ou grupo	Na caixa **Group (Grupo) ou User Names (nomes de usuário)**, selecione o usuário ou grupo que deseja alterar ou remover.

9. Execute as ações desejadas:

Se você quiser…	Faça o seguinte
Defina permissões NTFS padrão para um usuário ou grupo novo ou existente	Na caixa **Permissions for <Object>**, selecione as caixas **allow** ou **deny** para o tipo de acesso que você deseja permitir ou não permitir para o usuário ou grupo selecionado.
Remover um usuário ou grupo	Clique em **Remover**.

Se algumas ou todas as caixas de permissão padrão não forem selecionáveis, é porque as permissões são herdadas do objeto pai. A caixa **Special Permissions** não é selecionável. Se estiver selecionado, significa que um ou mais direitos avançados granulares foram definidos para o usuário ou grupo selecionado.

10. Depois de terminar de adicionar, remover ou editar permissões NTFS nesse objeto, clique em **OK**.

Verifique o acesso do usuário

Você deve testar se os usuários configurados podem acessar o compartilhamento SMB e os arquivos nele contidos.

Passos

1. Em um cliente Windows, faça login como um dos usuários que agora tem acesso ao compartilhamento.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:
   a. Selecione uma letra **Drive**.
   b. Na caixa **pasta**, digite o nome do compartilhamento que você fornecerá aos usuários.

      Se o nome do servidor SMB for SMB_SERVER01 e o compartilhamento for chamado "'SHARE1", você digitaria `\\SMB_SERVER01\share1`.

   c. Clique em **Finish**.

   A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.
4. Crie um arquivo de teste, verifique se ele existe, escreva texto nele e remova o arquivo de teste.

Gerencie SMB com a CLI

Visão geral da SMB

Os recursos de acesso a arquivos ONTAP estão disponíveis para o protocolo SMB. Você pode habilitar um servidor CIFS, criar compartilhamentos e ativar serviços Microsoft.

SMB (bloco de mensagens de servidor) refere-se aos dialetos modernos do protocolo Common Internet File System (CIFS). Você ainda verá *CIFS* na interface de linha de comando (CLI) do ONTAP e nas ferramentas de gerenciamento do OnCommand.

Suporte ao servidor SMB

Visão geral do suporte ao servidor SMB

Você pode ativar e configurar servidores SMB em máquinas virtuais de armazenamento (SVMs) para permitir que os clientes SMB acessem arquivos no cluster.

- Cada SVM de dados no cluster pode ser vinculado a exatamente um domínio do active Directory.

- Os SVMs de dados não precisam estar vinculados ao mesmo domínio.
- Vários SVMs podem ser vinculados ao mesmo domínio.

Você deve configurar as SVMs e LIFs que você está usando para fornecer dados antes de criar um servidor SMB. Se sua rede de dados não for plana, talvez você também precise configurar IPspaces, domínios de broadcast e sub-redes.

Informações relacionadas

"Gerenciamento de rede"

Modificar servidores SMB

"Administração do sistema"

Versões e funcionalidade SMB compatíveis

O bloco de mensagens de servidor (SMB) é um protocolo de compartilhamento remoto de arquivos usado por clientes e servidores Microsoft Windows. No ONTAP 9, todas as versões SMB são suportadas; no entanto, o suporte padrão ao SMB 1,0 depende da versão do ONTAP. Você deve verificar se o servidor SMB do ONTAP suporta os clientes e a funcionalidade necessária no seu ambiente.

As informações mais recentes sobre quais clientes SMB e controladores de domínio o ONTAP suporta estão disponíveis na *ferramenta Matriz de interoperabilidade*.

O SMB 2,0 e versões posteriores são ativados por padrão para servidores SMB do ONTAP 9 e podem ser ativados ou desativados conforme necessário. A tabela a seguir mostra o suporte ao SMB 1,0 e a configuração padrão.

Funcionalidade SMB 1,0:	**Nestes lançamentos do ONTAP 9:**			
	9,0	9,1	9,2	9,3 e mais tarde
Está ativado por predefinição	Sim	Sim	Sim	Não
Pode ser ativado ou desativado	Não	Sim * 9,1 P8 ou posterior necessário.	Sim	Sim

As configurações padrão para conexões SMB 1,0 e 2,0 para controladores de domínio também dependem da versão do ONTAP. Mais informações estão disponíveis na `vserver cifs security modify` página de manual. Para ambientes com servidores CIFS existentes que executam o SMB 1,0, você deve migrar para uma versão SMB posterior o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

A tabela a seguir mostra quais recursos SMB são suportados em cada versão SMB. Algumas funcionalidades SMB estão ativadas por predefinição e algumas requerem uma configuração adicional.

Esta funcionalidade:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
		1,0	2,0	2,1	3,0	3.1.1
Funcionalidade SMB 1,0 legada		X	X	X	X	X
Alças duráveis			X	X	X	X
Operações combinadas			X	X	X	X
Operações assíncronas			X	X	X	X
Tamanhos aumentados do buffer de leitura e gravação			X	X	X	X
Maior escalabilidade			X	X	X	X
Assinatura SMB	X	X	X	X	X	X
Formato de arquivo de fluxo de dados alternativo (ADS)	X	X	X	X	X	X
MTU grande (ativada por predefinição a partir de ONTAP 9.7)	X			X	X	X
Calços de leasing				X	X	X

Esta funcionalidade:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
Compartilhamentos disponíveis continuamente	X				X	X
Alças persistentes					X	X
Testemunha					X	X
CRIPTOGRAFIA SMB: AES-128-CCM	X				X	X
Escalabilidade horizontal (exigida pelos compartilhamentos da CA)					X	X
Failover transparente					X	X
Multicanal SMB (começando com ONTAP 9.4)	X				X	X
Integridade de pré-autenticação						X
Failover de cliente de cluster v,2 (CCFv2)						X
Criptografia SMB: AES-128-GCM (começando com ONTAP 9.1)	X					X

Informações relacionadas

Utilizar a assinatura SMB para melhorar a segurança da rede

Definir o nível mínimo de segurança de autenticação do servidor SMB

Configuração da criptografia SMB necessária em servidores SMB para transferências de dados por SMB

"Interoperabilidade do NetApp"

Recursos do Windows não suportados

Antes de usar o CIFS na rede, você precisa estar ciente de certos recursos do Windows que o ONTAP não oferece suporte.

O ONTAP não suporta os seguintes recursos do Windows:

- Sistema de arquivos criptografados (EFS)
- Registo de eventos do NT File System (NTFS) no diário de alterações
- Microsoft File Replication Service (FRS)
- Serviço de Indexação do Microsoft Windows
- Armazenamento remoto por meio do HSM (Hierarchical Storage Management)
- Gerenciamento de cotas de clientes Windows
- Semântica de cota do Windows
- O arquivo LMHOSTS
- Compactação nativa NTFS

Configure os serviços de nomes NIS ou LDAP no SVM

Com o acesso SMB, o mapeamento do usuário para um usuário UNIX é sempre realizado, mesmo quando você acessa dados em um volume de estilo de segurança NTFS. Se você mapear usuários do Windows para usuários UNIX correspondentes cujas informações são armazenadas em armazenamentos de diretório NIS ou LDAP ou se você usar LDAP para mapeamento de nomes, configure esses serviços de nomes durante a configuração SMB.

Antes de começar

Você precisa ter personalizado a configuração do banco de dados dos serviços de nomes para corresponder à infraestrutura do serviço de nomes.

Sobre esta tarefa

Os SVMs usam os bancos de dados ns-switch de serviços de nome para determinar a ordem na qual procurar as fontes para um determinado banco de dados de serviço de nome. A fonte ns-switch pode ser qualquer combinação de `files`, `nis`, ou `ldap`. Para o banco de dados de grupos, o ONTAP tenta obter as associações de grupos de todas as fontes configuradas e, em seguida, usa as informações de associação de grupo consolidado para verificações de acesso. Se uma dessas fontes não estiver disponível no momento da obtenção de informações do grupo UNIX, o ONTAP não poderá obter as credenciais UNIX completas e as verificações de acesso subsequentes poderão falhar. Portanto, você deve sempre verificar se todas as fontes do ns-switch estão configuradas para o banco de dados de grupo nas configurações do ns-switch.

O padrão é fazer com que o servidor SMB mapeie todos os usuários do Windows para o usuário UNIX padrão armazenado no banco de dados local `passwd`. Se você quiser usar a configuração padrão, a configuração de serviços de nome de usuário e grupo NIS ou LDAP UNIX ou mapeamento de usuário LDAP é opcional para o acesso SMB.

Passos

1. Se as informações de usuário, grupo e netgroup UNIX forem gerenciadas por serviços de nome NIS, configure os serviços de nome NIS:

   a. Determine a ordem atual dos serviços de nome usando o `vserver services name-service ns-switch show` comando.

      Neste exemplo, os três bancos de dados (`group`, `passwd` e `netgroup`) que podem ser usados `nis` como uma fonte de serviço de nomes estão usando `files` apenas como uma fonte.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                  Source
      Vserver         Database       Enabled      Order
      --------------- ------------   ---------    ---------
      vs1             hosts          true         dns,
                                                  files
      vs1             group          true         files
      vs1             passwd         true         files
      vs1             netgroup       true         files
      vs1             namemap        true         files
      ```

      Você deve adicionar a `nis` fonte `group` aos bancos de dados e `passwd`, opcionalmente, ao `netgroup` banco de dados.

   b. Ajuste a ordenação do banco de dados ns-switch do serviço de nomes conforme desejado usando o `vserver services name-service ns-switch modify` comando.

      Para obter a melhor performance, você não deve adicionar um serviço de nomes a um banco de dados de serviços de nomes, a menos que se Planeje configurar esse serviço de nomes no SVM.

      Se você modificar a configuração para mais de um banco de dados de serviço de nome, deverá executar o comando separadamente para cada banco de dados de serviço de nome que deseja modificar.

      Neste exemplo, `nis` e `files` são configurados como fontes para os `group` bancos de dados e `passwd`, nessa ordem. O restante dos bancos de dados do serviço de nomes não foi alterado.

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database group
      -sources nis,files vserver services name-service ns-switch modify -vserver
      vs1 -database passwd -sources nis,files
      ```

   c. Verifique se a ordem dos serviços de nome está correta usando o `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                    Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. Crie a configuração do serviço de nomes NIS
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

`vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60`

> A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

e. Verifique se o serviço de nomes NIS está configurado corretamente: `vserver services name-service nis-domain show vserver <vserver_name>`

`vserver services name-service nis-domain show vserver vs1`

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. Se as informações de usuário, grupo e netgroup UNIX ou mapeamento de nomes for gerenciado por serviços de nomes LDAP, configure os serviços de nomes LDAP usando as informações localizadas "Gerenciamento de NFS".

Como funciona a configuração do switch do serviço de nomes ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

Tipo de banco de dados	Define fontes de serviço de nome para…	Fontes válidas são…
hosts	Conversão de nomes de host para endereços IP	ficheiros, dns
grupo	Procurar informações do grupo de utilizadores	arquivos, nis, ldap
passwd	Procurar informações do utilizador	arquivos, nis, ldap
grupo de rede	Procurar informações do netgroup	arquivos, nis, ldap
namemap	Mapeando nomes de usuários	ficheiros, ldap

Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

Especificar tipo de origem…	Para procurar informações em…	Gerenciado pelas famílias de comando…

ficheiros	Arquivos de origem local	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	`vserver services name-service ldap`
dns	Servidores DNS externos conforme especificado na configuração DNS do SVM	`vserver services name-service dns`

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

Fonte do serviço de nomes externo	Protocolo utilizado para acesso
NIS	UDP
DNS	UDP
LDAP	TCP

Exemplo

O exemplo a seguir exibe a configuração do switch de serviço de nomes para o SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM.svm_1. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

Gerenciar servidores SMB

Modificar servidores SMB

Pode mover um servidor SMB de um grupo de trabalho para um domínio do ative Directory, de um grupo de trabalho para outro grupo de trabalho ou de um domínio do ative Directory para um grupo de trabalho utilizando o `vserver cifs modify` comando.

Sobre esta tarefa

Você também pode modificar outros atributos do servidor SMB, como o nome do servidor SMB e o status administrativo. Consulte a página de manual para obter detalhes.

Opções

- Mova o servidor SMB de um grupo de trabalho para um domínio do ative Directory:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Mova o servidor SMB do grupo de trabalho para um domínio do ative Directory: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  Para criar uma conta de máquina do ative Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=`*`example`* `ou` contentor dentro do *`example`* domínio .com.

  A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

- Mover o servidor SMB de um grupo de trabalho para outro grupo de trabalho:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Modifique o grupo de trabalho para o servidor SMB: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Mova o servidor SMB de um domínio do ative Directory para um grupo de trabalho:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Mova o servidor SMB do domínio do ative Directory para um grupo de trabalho: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

  ```
  cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
  ```

Para entrar no modo de grupo de trabalho, todos os recursos baseados em domínio devem ser desativados e suas configurações removidas automaticamente pelo sistema, incluindo compartilhamentos continuamente disponíveis, cópias de sombra e AES. No entanto, as ACLs de compartilhamento configuradas por domínio, como "EXAMPLE.COM\userName", não funcionarão corretamente, mas não poderão ser removidas pelo ONTAP. Remova essas ACLs de compartilhamento o mais rápido possível usando ferramentas externas após a conclusão do comando. Se o AES estiver ativado, você poderá ser solicitado a fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para desativá-lo no domínio "example.com".

- Modifique outros atributos usando o parâmetro apropriado do `vserver cifs modify` comando.

Use as opções para personalizar servidores SMB

Opções de servidor SMB disponíveis

É útil saber quais opções estão disponíveis ao considerar como personalizar o servidor SMB. Embora algumas opções sejam para uso geral no servidor SMB, várias são usadas para ativar e configurar a funcionalidade SMB específica. As opções de servidor SMB são controladas com a `vserver cifs options modify` opção.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível de privilégio de administrador:

- **Configurando o valor de tempo limite da sessão SMB**

  Configurar esta opção permite especificar o número de segundos de tempo ocioso antes de uma sessão SMB ser desconetada. Uma sessão ociosa é uma sessão na qual um usuário não tem arquivos ou diretórios abertos no cliente. O valor padrão é de 900 segundos.

- **Configurando o usuário UNIX padrão**

  Configurar esta opção permite especificar o utilizador UNIX predefinido que o servidor SMB utiliza. O ONTAP cria automaticamente um usuário padrão chamado "'pcuser'" (com um UID de 65534), cria um grupo chamado "'pcuser'" (com um GID de 65534) e adiciona o usuário padrão ao grupo "'pcuser'". Quando você cria um servidor SMB, o ONTAP configura automaticamente "'pcuser'" como o usuário UNIX padrão.

- **Configurando o usuário UNIX convidado**

  A configuração desta opção permite especificar o nome de um usuário UNIX ao qual os usuários que fazem login de domínios não confiáveis são mapeados, o que permite que um usuário de um domínio não confiável se conete ao servidor SMB. Por padrão, essa opção não está configurada (não há valor padrão); portanto, o padrão é não permitir que usuários de domínios não confiáveis se conetem ao servidor SMB.

- * Ativar ou desativar a execução de concessão de leitura para bits de modo*

  Ativar ou desativar esta opção permite que você especifique se deseja permitir que clientes SMB executem arquivos executáveis com bits de modo UNIX aos quais eles têm acesso de leitura, mesmo quando o bit executável UNIX não está definido. Esta opção está desativada por predefinição.

- **Ativar ou desativar a capacidade de eliminar ficheiros só de leitura de clientes NFS**

Ativar ou desativar esta opção determina se os clientes NFS devem excluir arquivos ou pastas com o conjunto de atributos somente leitura. A semântica de exclusão NTFS não permite a exclusão de um arquivo ou pasta quando o atributo somente leitura é definido. A semântica de exclusão do UNIX ignora o bit somente leitura, usando as permissões do diretório pai para determinar se um arquivo ou pasta pode ser excluído. A configuração padrão é `disabled`, o que resulta em semântica de exclusão NTFS.

- **Configurando endereços de servidor do Windows Internet Name Service**

  Configurar esta opção permite especificar uma lista de endereços de servidor WINS (Serviço de nomes de Internet do Windows) como uma lista delimitada por vírgulas. Você deve especificar endereços IPv4. Os endereços IPv6 não são suportados. Não há valor padrão.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível avançado de privilégio:

- **Concessão de permissões de grupo UNIX para usuários CIFS**

  Configurar esta opção determina se o usuário CIFS de entrada que não é o proprietário do arquivo pode receber a permissão de grupo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `true`, a permissão de grupo será concedida para o arquivo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `false`, as regras UNIX normais serão aplicáveis para conceder a permissão de arquivo. Este parâmetro é aplicável a arquivos de estilo de segurança UNIX que têm permissão definida como `mode bits` e não é aplicável a arquivos com o modo de segurança NTFS ou NFSv4. A predefinição é `false`.

- **Ativar ou desativar o SMB 1,0**

  O SMB 1,0 é desativado por padrão em uma SVM para a qual um servidor SMB é criado no ONTAP 9.3.

  > ⓘ A partir do ONTAP 9.3, o SMB 1,0 é desativado por padrão para novos servidores SMB criados no ONTAP 9.3. Você deve migrar para uma versão SMB mais recente o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

- **Ativar ou desativar o SMB 2.x**

  SMB 2,0 é a versão mínima de SMB que suporta failover de LIF. Se desativar o SMB 2.x, o ONTAP também desativa automaticamente o SMB 3.X.

  O SMB 2,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,0**

  O SMB 3,0 é a versão mínima para SMB compatível com compartilhamentos disponíveis continuamente. O Windows Server 2012 e o Windows 8 são as versões mínimas do Windows que suportam SMB 3,0.

  O SMB 3,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,1**

  O Windows 10 é a única versão do Windows que suporta SMB 3,1.

  O SMB 3,1 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- * Ativar ou desativar a descarga de cópia ODX*

  O descarregamento de cópia ODX é usado automaticamente por clientes Windows que o suportam. Esta opção está ativada por predefinição.

- * Ativar ou desativar o mecanismo de cópia direta para descarga de cópia ODX*

  O mecanismo de cópia direta aumenta o desempenho da operação de descarga de cópia quando os clientes do Windows tentam abrir o arquivo de origem de uma cópia em um modo que impede que o arquivo seja alterado enquanto a cópia está em andamento. Por padrão, o mecanismo de cópia direta está ativado.

- * Ativar ou desativar referências automáticas de nós*

  Com referências automáticas de nós, o servidor SMB refere automaticamente os clientes a um data LIF local para o nó que hospeda os dados acessados através do compartilhamento solicitado.

- **Ativar ou desativar políticas de exportação para SMB**

  Esta opção está desativada por predefinição.

- * Ativar ou desativar usando pontos de junção como pontos de reparação*

  Se esta opção estiver ativada, o servidor SMB expõe pontos de junção para clientes SMB como pontos de reparação. Esta opção é válida apenas para ligações SMB 2.x ou SMB 3,0. Esta opção está ativada por predefinição.

  Esta opção é suportada apenas em SVMs. A opção é ativada por padrão em SVMs

- **Configurando o número máximo de operações simultâneas por conexão TCP**

  O valor padrão é 255.

- **Ativar ou desativar a funcionalidade de grupos e utilizadores locais do Windows**

  Esta opção está ativada por predefinição.

- **Ativar ou desativar a autenticação de utilizadores locais do Windows**

  Esta opção está ativada por predefinição.

- * Ativar ou desativar a funcionalidade de cópia de sombra VSS*

  O ONTAP usa a funcionalidade de cópia de sombra para executar backups remotos de dados armazenados usando a solução Hyper-V sobre SMB.

  Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- **Configurando a profundidade do diretório de cópia de sombra**

  A configuração desta opção permite definir a profundidade máxima dos diretórios para criar cópias de sombra ao usar a funcionalidade de cópia de sombra.

  Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- * Ativar ou desativar recursos de pesquisa de vários domínios para mapeamento de nomes*

  Se ativado, quando um usuário UNIX é mapeado para um usuário de domínio do Windows usando um curinga (*) na parte de domínio do nome de usuário do Windows (por exemplo, * / joe), o ONTAP procura o usuário especificado em todos os domínios com confiança bidirecional para o domínio doméstico. O domínio inicial é o domínio que contém a conta de computador do servidor SMB.

  Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Se esta opção estiver ativada e uma lista de preferências estiver configurada, a lista de preferências será utilizada para efetuar pesquisas de mapeamento de nomes de vários domínios.

  O padrão é habilitar pesquisas de mapeamento de nomes de vários domínios.

- **Configurando o tamanho do setor do sistema de arquivos**

  A configuração desta opção permite configurar o tamanho do setor do sistema de arquivos em bytes que o ONTAP reporta para clientes SMB. Existem dois valores válidos para esta opção: `4096` E `512`. O valor padrão é `4096`. Talvez seja necessário definir esse valor `512` se o aplicativo Windows suportar apenas um tamanho de setor de 512 bytes.

- **Ativar ou desativar o controlo de Acesso Dinâmico**

  Ativar esta opção permite proteger objetos no servidor SMB utilizando o controlo de Acesso Dinâmico (DAC), incluindo a utilização de auditoria para encenar políticas de acesso centrais e utilizar objetos de Diretiva de Grupo para implementar políticas de acesso centrais. A opção está desativada por predefinição.

  Esta opção é suportada apenas em SVMs.

- * Definir as restrições de acesso para sessões não autenticadas (restringir anônimo)*

  Definir esta opção determina quais são as restrições de acesso para sessões não autenticadas. As restrições são aplicadas a usuários anônimos. Por padrão, não há restrições de acesso para usuários anônimos.

- * Ativar ou desativar a apresentação de ACLs NTFS em volumes com segurança eficaz UNIX (volumes estilo de segurança UNIX ou volumes mistos estilo de segurança com segurança eficaz UNIX)*

  Ativar ou desativar esta opção determina como a segurança de arquivos em arquivos e pastas com segurança UNIX é apresentada aos clientes SMB. Se ativado, o ONTAP apresenta arquivos e pastas em volumes com segurança UNIX para clientes SMB como tendo segurança de arquivos NTFS com ACLs NTFS. Se desativado, o ONTAP apresenta volumes com segurança UNIX como volumes FAT, sem segurança de arquivos. Por padrão, os volumes são apresentados como tendo segurança de arquivos NTFS com ACLs NTFS.

- * Habilitando ou desativando a funcionalidade de abertura falsa do SMB*

  A ativação dessa funcionalidade melhora o desempenho do SMB 2.x e do SMB 3,0, otimizando como o ONTAP faz solicitações abertas e fechadas ao consultar informações de atributos em arquivos e diretórios. Por padrão, a funcionalidade de abertura falsa do SMB está ativada. Essa opção é útil somente para conexões feitas com SMB 2.x ou posterior.

- * Ativar ou desativar as extensões UNIX*

Ativar esta opção ativa extensões UNIX num servidor SMB. As extensões UNIX permitem que a segurança de estilo POSIX/UNIX seja exibida através do protocolo SMB. Por predefinição, esta opção está desativada.

Se você tiver clientes SMB baseados em UNIX, como clientes Mac OSX, em seu ambiente, você deve habilitar extensões UNIX. A habilitação de extensões UNIX permite que o servidor SMB transmita informações de segurança POSIX/UNIX sobre SMB para o cliente baseado em UNIX, o que converte as informações de segurança em segurança POSIX/UNIX.

- * Ativar ou desativar o suporte para pesquisas de nomes curtos*

  Ativar esta opção permite que o servidor SMB realize pesquisas em nomes curtos. Uma consulta de pesquisa com esta opção ativada tenta corresponder a nomes de arquivo 8,3 juntamente com nomes de arquivo longos. O valor padrão para este parâmetro é `false`.

- * Ativar ou desativar o suporte para publicidade automática de capacidades DFS*

  Ativar ou desativar esta opção determina se os servidores SMB anunciam automaticamente os recursos DFS para clientes SMB 2.x e SMB 3,0 que se conetam a compartilhamentos. O ONTAP usa referências DFS na implementação de links simbólicos para acesso SMB. Se ativado, o servidor SMB sempre anuncia recursos DFS, independentemente de o acesso a links simbólicos estar habilitado. Se estiver desativado, o servidor SMB anunciará os recursos DFS somente quando os clientes se conetarem a compartilhamentos onde o acesso ao link simbólico está habilitado.

- **Configurando o número máximo de créditos SMB**

  A partir do ONTAP 9.4, a configuração da `-max-credits` opção permite limitar o número de créditos a serem concedidos em uma conexão SMB quando clientes e servidor estão executando o SMB versão 2 ou posterior. O valor padrão é 128.

- * Ativar ou desativar o suporte para SMB Multichannel*

  Ativar a `-is-multichannel-enabled` opção no ONTAP 9.4 e versões posteriores permite que o servidor SMB estabeleça várias conexões para uma única sessão SMB quando as NICs apropriadas são implantadas no cluster e em seus clientes. Isso melhora a taxa de transferência e a tolerância a falhas. O valor padrão para este parâmetro é `false`.

  Quando o Multichannel SMB está ativado, você também pode especificar os seguintes parâmetros:

  - O número máximo de conexões permitido por sessão multicanal. O valor padrão para este parâmetro é 32.
  - O número máximo de interfaces de rede anunciadas por sessão multicanal. O valor padrão para este parâmetro é 256.

Configurando opções de servidor SMB

Você pode configurar as opções de servidor SMB a qualquer momento depois de criar um servidor SMB em uma máquina virtual de storage (SVM).

Passo

1. Execute a ação desejada:

Se pretender configurar as opções do servidor SMB…	Digite o comando…
No nível de privilégios de administrador	`vserver cifs options modify -vserver` *`vserver_name options`*
Em nível avançado de privilégios	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Para obter mais informações sobre como configurar as opções do servidor SMB, consulte a página de manual do `vserver cifs options modify` comando.

Configure a permissão Grant UNIX group para usuários SMB

Você pode configurar essa opção para conceder permissões de grupo para acessar arquivos ou diretórios, mesmo que o usuário SMB de entrada não seja o proprietário do arquivo.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a permissão Grant UNIX group conforme apropriado:

Se você quiser	Introduza o comando
Ative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	`vserver cifs options modify –grant-unix-group-perms-to-others true`
Desative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Configurar restrições de acesso para usuários anônimos

Por padrão, um usuário anônimo e não autenticado (também conhecido como *null user*) pode acessar certas informações na rede. Você pode usar uma opção de servidor SMB para configurar restrições de acesso para o usuário anônimo.

Sobre esta tarefa

A `-restrict-anonymous` opção servidor SMB corresponde à `RestrictAnonymous` entrada do Registro no Windows.

Os usuários anônimos podem listar ou enumerar certos tipos de informações de sistema de hosts do Windows na rede, incluindo nomes e detalhes de usuários, políticas de conta e nomes de compartilhamento. Você pode controlar o acesso para o usuário anônimo especificando uma das três configurações de restrição de acesso:

Valor	Descrição
`no-restriction` (predefinição)	Não especifica restrições de acesso para usuários anônimos.
`no-enumeration`	Especifica que somente a enumeração é restrita para usuários anônimos.
`no-access`	Especifica que o acesso é restrito para usuários anônimos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração restringir anônimo: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor SMB disponíveis

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para dados de estilo de segurança UNIX

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para visão geral de dados em estilo de segurança UNIX

Você pode escolher como deseja apresentar a segurança de arquivos a clientes SMB para dados de estilo de segurança UNIX ativando ou desativando a apresentação de ACLs NTFS para clientes SMB. Há vantagens em cada configuração, que você deve entender para escolher a configuração mais adequada para seus requisitos de negócios.

Por padrão, o ONTAP apresenta permissões UNIX em volumes estilo de segurança UNIX para clientes SMB como ACLs NTFS. Existem cenários em que isso é desejável, incluindo o seguinte:

- Você deseja exibir e editar permissões UNIX usando a guia **Segurança** na caixa Propriedades do Windows.

  Não é possível modificar permissões de um cliente Windows se a operação não for permitida pelo sistema UNIX. Por exemplo, você não pode alterar a propriedade de um arquivo que você não possui, porque o sistema UNIX não permite essa operação. Essa restrição impede que clientes SMB ignorem permissões UNIX definidas nos arquivos e pastas.

- Os usuários estão editando e salvando arquivos no volume estilo de segurança UNIX usando certos aplicativos do Windows, por exemplo, Microsoft Office, onde o ONTAP deve preservar permissões UNIX durante operações de salvamento.

- Existem certos aplicativos do Windows no seu ambiente que esperam ler ACLs NTFS em arquivos que usam.

Em certas circunstâncias, você pode querer desativar a apresentação de permissões UNIX como ACLs NTFS. Se esta funcionalidade estiver desativada, o ONTAP apresenta volumes de estilo de segurança UNIX como volumes FAT para clientes SMB. Existem razões específicas pelas quais você pode querer apresentar volumes de estilo de segurança UNIX como volumes FAT para clientes SMB:

- Você só altera permissões UNIX usando montagens em clientes UNIX.

  A guia Segurança não está disponível quando um volume de estilo de segurança UNIX é mapeado em um cliente SMB. A unidade mapeada parece ser formatada com o sistema de arquivos FAT, que não tem permissões de arquivo.

- Você está usando aplicativos sobre SMB que definem ACLs NTFS em arquivos e pastas acessados, o que pode falhar se os dados residirem em volumes de estilo de segurança UNIX.

  Se o ONTAP relatar o volume como FAT, o aplicativo não tenta alterar uma ACL.

Informações relacionadas

Configurando estilos de segurança no FlexVol volumes

Configurando estilos de segurança no qtrees

Ative ou desative a apresentação de ACLs NTFS para dados de estilo de segurança UNIX

Você pode ativar ou desativar a apresentação de ACLs NTFS para clientes SMB para dados de estilo de segurança UNIX (volumes de estilo de segurança UNIX e volumes mistos de estilo de segurança com segurança efetiva UNIX).

Sobre esta tarefa

Se você ativar essa opção, o ONTAP apresenta arquivos e pastas em volumes com estilo de segurança UNIX eficaz para clientes SMB como tendo ACLs NTFS. Se desativar esta opção, os volumes são apresentados como volumes FAT para clientes SMB. O padrão é apresentar ACLs NTFS a clientes SMB.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração da opção ACL NTFS UNIX: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de

segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

  Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

  Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Gerenciar configurações de segurança do servidor SMB

Como o ONTAP lida com a autenticação de cliente SMB

Antes que os usuários possam criar conexões SMB para acessar dados contidos no SVM, elas devem ser autenticadas pelo domínio ao qual o servidor SMB pertence. O servidor SMB suporta dois métodos de autenticação, Kerberos e NTLM (NTLMv1 ou

NTLMv2). Kerberos é o método padrão usado para autenticar usuários de domínio.

Autenticação Kerberos

O ONTAP oferece suporte à autenticação Kerberos ao criar sessões SMB autenticadas.

Kerberos é o serviço de autenticação principal do ative Directory. O servidor Kerberos, ou serviço KDC (Centro de distribuição de chaves Kerberos), armazena e recupera informações sobre princípios de segurança no ative Directory. Ao contrário do modelo NTLM, os clientes do ative Directory que desejam estabelecer uma sessão com outro computador, como o servidor SMB, contatam diretamente um KDC para obter suas credenciais de sessão.

Autenticação NTLM

A autenticação de cliente NTLM é feita usando um protocolo de resposta de desafio baseado no conhecimento compartilhado de um segredo específico do usuário com base em uma senha.

Se um usuário criar uma conexão SMB usando uma conta de usuário local do Windows, a autenticação é feita localmente pelo servidor SMB usando NTLMv2.

Diretrizes para configurações de segurança de servidor SMB em uma configuração de recuperação de desastres SVM

Antes de criar um SVM configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), você deve saber como as configurações de segurança do servidor SMB são gerenciadas no SVM de destino.

- As configurações de segurança de servidor SMB não padrão não são replicadas para o destino.

  Quando você cria um servidor SMB no SVM de destino, todas as configurações de segurança do servidor SMB são definidas como valores padrão. Quando o destino de recuperação de desastres da SVM é inicializado, atualizado ou ressincido, as configurações de segurança do servidor SMB na origem não são replicadas para o destino.

- Você deve configurar manualmente configurações de segurança de servidor SMB não padrão.

  Se você tiver configurações de segurança de servidor SMB não padrão configuradas no SVM de origem, será necessário configurar manualmente essas mesmas configurações no SVM de destino depois que o destino se tornar leitura-gravação (depois que a relação SnapMirror for interrompida).

Exibir informações sobre as configurações de segurança do servidor SMB

Você pode exibir informações sobre as configurações de segurança do servidor SMB em suas máquinas virtuais de armazenamento (SVMs). Pode utilizar estas informações para verificar se as definições de segurança estão corretas.

Sobre esta tarefa

Uma configuração de segurança exibida pode ser o valor padrão para esse objeto ou um valor não padrão configurado usando a CLI do ONTAP ou usando objetos de diretiva de grupo (GPOs) do ative Directory.

Não use o `vserver cifs security show` comando para servidores SMB no modo de grupo de trabalho, porque algumas das opções não são válidas.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Todas as configurações de segurança em uma SVM especificada	`vserver cifs security show -vserver` *`vserver_name`*
Configurações ou configurações de segurança específicas no SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Você pode inserir `-fields ?` para determinar quais campos você pode usar.

Exemplo

O exemplo a seguir mostra todas as configurações de segurança do SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:       false
                         LM Compatibility Level:       lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:       false
                        Client Session Security:       none
               SMB1 Enabled for DC Connections:        false
               SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:         false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:         false
 AES session key enabled for NetLogon channel:         false
  Try Channel Binding For AD LDAP Connections:         false
```

Observe que as configurações exibidas dependem da versão do ONTAP em execução.

O exemplo a seguir mostra a inclinação do relógio Kerberos para SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Ative ou desative a complexidade de senha necessária para usuários SMB locais

A complexidade de senha necessária fornece segurança aprimorada para usuários locais de SMB em suas máquinas virtuais de armazenamento (SVMs). A funcionalidade de complexidade de palavra-passe necessária está ativada por predefinição. Você pode desativá-lo e reativá-lo a qualquer momento.

Antes de começar

Usuários locais, grupos locais e autenticação de usuário local devem estar habilitados no servidor CIFS.

Sobre esta tarefa

Você não deve usar o `vserver cifs security modify` comando para um servidor CIFS no modo de grupo de trabalho porque algumas das opções não são válidas.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a complexidade de senha necessária para usuários SMB locais seja…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Verifique a configuração de segurança para a complexidade necessária da senha: `vserver cifs security show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir mostra que a complexidade de senha necessária está habilitada para usuários SMB locais para SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Informações relacionadas

Exibindo informações sobre as configurações de segurança do servidor CIFS

Usando usuários locais e grupos para autenticação e autorização

Requisitos para senhas de usuários locais

Alterando senhas de contas de usuário locais

Modifique as configurações de segurança Kerberos do servidor CIFS

Você pode modificar certas configurações de segurança Kerberos do servidor CIFS, incluindo o tempo máximo permitido de distorção do relógio Kerberos, a vida útil do ticket Kerberos e o número máximo de dias de renovação de ticket.

Sobre esta tarefa

Modificar as configurações do Kerberos do servidor CIFS usando o `vserver cifs security modify` comando modifica as configurações somente na máquina virtual de armazenamento (SVM) única que você especificar com o `-vserver` parâmetro. Você pode gerenciar centralmente as configurações de segurança Kerberos para todos os SVMs no cluster que pertencem ao mesmo domínio do ative Directory usando os GPOs (objetos de diretiva de grupo) do ative Directory.

Passos

1. Execute uma ou mais das seguintes ações:

Se você quiser…	Digite…
Especifique o tempo máximo permitido de distorção do relógio Kerberos em minutos (9.13.1 e posterior) ou segundos (9.12.1 ou anterior).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* A predefinição é 5 minutos.
Especifique a vida útil do ticket Kerberos em horas.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` A predefinição é 10 horas.

Especifique o número máximo de dias de renovação do ticket.	`vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days` A configuração padrão é de 7 dias.
Especifique o tempo limite para sockets em KDCs após o qual todos os KDCs são marcados como inalcançáveis.	`vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds` A predefinição é 3 segundos.

2. Verifique as configurações de segurança do Kerberos:

   `vserver cifs security show -vserver vserver_name`

Exemplo

O exemplo a seguir faz as seguintes alterações na segurança Kerberos: "'Kerberos Clock Skew'" está definido como 3 minutos e "'Kerberos Ticket Age'" está definido como 8 horas para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
         Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

Informações relacionadas

"Exibindo informações sobre as configurações de segurança do servidor CIFS"

"GPOs compatíveis"

"Aplicando objetos de Diretiva de Grupo a servidores CIFS"

Defina o nível mínimo de segurança de autenticação do servidor SMB

Você pode definir o nível mínimo de segurança do servidor SMB, também conhecido como *LMCompatibilityLevel*, em seu servidor SMB para atender aos requisitos de segurança da sua empresa para acesso ao cliente SMB. O nível mínimo de segurança é o nível mínimo dos tokens de segurança que o servidor SMB aceita de clientes SMB.

Sobre esta tarefa

- Os servidores SMB no modo de grupo de trabalho suportam apenas a autenticação NTLM. A autenticação Kerberos não é suportada.
- LMCompatibilityLevel aplica-se apenas à autenticação de cliente SMB, não à autenticação de administrador.

Você pode definir o nível mínimo de segurança de autenticação para um dos quatro níveis de segurança suportados.

Valor	Descrição
`lm-ntlm-ntlmv2-krb` (predefinição)	A máquina virtual de armazenamento (SVM) aceita segurança de autenticação LM, NTLM, NTLMv2 e Kerberos.
`ntlm-ntlmv2-krb`	O SVM aceita segurança de autenticação NTLM, NTLMv2 e Kerberos. O SVM nega a autenticação LM.
`ntlmv2-krb`	O SVM aceita a segurança de autenticação NTLMv2 e Kerberos. O SVM nega a autenticação LM e NTLM.
`krb`	O SVM aceita apenas a segurança de autenticação Kerberos. O SVM nega a autenticação LM, NTLM e NTLMv2.

Passos

1. Defina o nível mínimo de segurança de autenticação: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verifique se o nível de segurança de autenticação está definido para o nível desejado: `vserver cifs security show -vserver` *`vserver_name`*

Informações relacionadas

Ativar ou desativar a encriptação AES para comunicação baseada no Kerberos

Configurar segurança forte para comunicação baseada no Kerberos usando criptografia AES

Para uma segurança mais forte com comunicação baseada no Kerberos, é possível ativar a criptografia AES-256 e AES-128 no servidor SMB. Por padrão, quando você cria um servidor SMB no SVM, a criptografia AES (Advanced Encryption Standard) é desativada. Você deve habilitá-lo para aproveitar a segurança forte fornecida pela

criptografia AES.

A comunicação relacionada ao Kerberos para SMB é usada durante a criação do servidor SMB na SVM, bem como durante a fase de configuração da sessão SMB. O servidor SMB suporta os seguintes tipos de criptografia para comunicação Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Se você quiser usar o tipo de criptografia de segurança mais alto para comunicação Kerberos, ative a criptografia AES para comunicação Kerberos no SVM.

Quando o servidor SMB é criado, o controlador de domínio cria uma conta de máquina de computador no ative Directory. Neste momento, o KDC se torna ciente dos recursos de criptografia da conta de máquina específica. Posteriormente, um tipo de criptografia específico é selecionado para criptografar o ticket de serviço que o cliente apresenta ao servidor durante a autenticação.

A partir do ONTAP 9.12,1, você pode especificar quais tipos de criptografia anunciar no KDC do ative Directory (AD). Pode utilizar a `-advertised-enc-types` opção para ativar os tipos de encriptação recomendados e pode utilizá-la para desativar os tipos de encriptação mais fracos. Aprenda a "Ative e desative os tipos de criptografia para comunicação baseada no Kerberos".

> As novas instruções Intel AES (Intel AES NI) estão disponíveis no SMB 3,0, melhorando o algoritmo AES e acelerando a criptografia de dados com famílias de processadores suportadas.começando com SMB 3,1.1, AES-128-GCM substitui AES-128-CCM como o algoritmo hash usado pela criptografia SMB.

Informações relacionadas

Modificação das configurações de segurança Kerberos do servidor CIFS

Ativar ou desativar a encriptação AES para comunicação baseada no Kerberos

Para aproveitar a segurança mais forte com a comunicação baseada no Kerberos, você deve usar a criptografia AES-256 e AES-128 no servidor SMB. A partir do ONTAP 9.13,1, a encriptação AES é ativada por predefinição. Se você não quiser que o servidor SMB selecione os tipos de criptografia AES para comunicação baseada em Kerberos com o KDC do ative Directory (AD), você pode desativar a criptografia AES.

Se a encriptação AES está ativada por predefinição e se tem a opção de especificar tipos de encriptação depende da versão do ONTAP.

Versão de ONTAP	A encriptação AES está ativada …	Você pode especificar tipos de criptografia?
9.13.1 e mais tarde	Por padrão	Sim
9.12.1	Manualmente	Sim
9.11.1 e anteriores	Manualmente	Não

A partir do ONTAP 9.12,1, a criptografia AES é ativada e desativada usando a `-advertised-enc-types` opção, que permite especificar os tipos de criptografia anunciados para o AD KDC. A configuração padrão é `rc4` e `des`, mas quando um tipo AES é especificado, a criptografia AES é ativada. Você também pode usar a opção para desativar explicitamente os tipos de criptografia RC4 e DES mais fracos. No ONTAP 9.11,1 e anterior, você deve usar a `-is-aes-encryption-enabled` opção para ativar e desativar a criptografia AES e os tipos de criptografia não podem ser especificados.

Para melhorar a segurança, a máquina virtual de armazenamento (SVM) altera a senha da conta de máquina no AD sempre que a opção de segurança AES é modificada. A alteração da senha pode exigir credenciais administrativas do AD para a unidade organizacional (ou) que contém a conta da máquina.

Se um SVM for configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), as configurações de segurança do servidor SMB não padrão não serão replicadas para o destino. Se você ativou a criptografia AES no SVM de origem, será necessário habilitá-la manualmente.

Exemplo 10. Passos

ONTAP 9.12,1 e posterior

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Desativado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Nota: a `-is-aes-encryption-enabled` opção está obsoleta no ONTAP 9.12,1 e pode ser removida em uma versão posterior.

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11,1 e anteriores

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Desativado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   O `is-aes-encryption-enabled` campo é exibido `true` se a criptografia AES estiver ativada e `false` se estiver desativada.

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Informações relacionadas

"O usuário de domínio não consegue fazer login no cluster com Domain-Tunnel"

Utilize a assinatura SMB para melhorar a segurança da rede

Utilize a assinatura SMB para melhorar a visão geral da segurança da rede

A assinatura SMB ajuda a garantir que o tráfego de rede entre o servidor SMB e o cliente não seja comprometido; isso evita ataques de repetição. Por padrão, o ONTAP oferece suporte à assinatura SMB quando solicitado pelo cliente. Opcionalmente, o administrador de armazenamento pode configurar o servidor SMB para exigir assinatura SMB.

Como as políticas de assinatura SMB afetam a comunicação com um servidor CIFS

Além das configurações de segurança de assinatura SMB do servidor CIFS, duas diretivas de assinatura SMB em clientes Windows controlam a assinatura digital de comunicações entre clientes e o servidor CIFS. Você pode configurar a configuração que atende aos requisitos da sua empresa.

As diretivas SMB do cliente são controladas por meio das configurações de diretiva de segurança local do Windows, que são configuradas usando o MMC (Console de Gerenciamento da Microsoft) ou GPOs do ative Directory. Para obter mais informações sobre a assinatura SMB do cliente e problemas de segurança, consulte a documentação do Microsoft Windows.

Aqui estão descrições das duas políticas de assinatura SMB em clientes Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Esta configuração controla se a capacidade de assinatura SMB do cliente está ativada. Ele é habilitado por padrão. Quando essa configuração é desativada no cliente, as comunicações do cliente com o servidor CIFS dependem da configuração de assinatura SMB no servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Esta configuração controla se o cliente requer assinatura SMB para se comunicar com um servidor. Ele está desativado por padrão. Quando essa configuração é desativada no cliente, o comportamento de assinatura SMB é baseado na configuração de diretiva `Microsoft network client: Digitally sign communications (if server agrees)` e na configuração no servidor CIFS.

> Se o seu ambiente incluir clientes Windows configurados para exigir assinatura SMB, você deverá ativar a assinatura SMB no servidor CIFS. Se você não fizer isso, o servidor CIFS não poderá fornecer dados a esses sistemas.

Os resultados efetivos das configurações de assinatura SMB do cliente e do servidor CIFS dependem se as sessões SMB usam SMB 1,0 ou SMB 2.x e posterior.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 1,0:

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura desativada e não necessária	Não assinado	Assinado
Assinatura ativada e não necessária	Não assinado	Assinado
Assinatura desativada e necessária	Assinado	Assinado
Assinatura ativada e necessária	Assinado	Assinado

Clientes Windows SMB 1 mais antigos e alguns clientes SMB 1 não Windows podem não conseguir se conetar se a assinatura estiver desativada no cliente, mas necessária no servidor CIFS.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 2.x ou SMB 3,0:

Para clientes SMB 2.x e SMB 3,0, a assinatura SMB está sempre ativada. Não pode ser desativado.

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura não necessária	Não assinado	Assinado
Assinatura necessária	Assinado	Assinado

A tabela a seguir resume o comportamento padrão de assinatura SMB de cliente e servidor da Microsoft:

Protocolo	Algoritmo hash	Pode ativar/desativar	Pode exigir/não exigir	Padrão do cliente	Padrão do servidor	DC predefinido
SMB 1,0	MD5	Sim	Sim	Ativado (não necessário)	Desativado (não necessário)	Obrigatório
SMB 2.x	HMAC SHA-256	Não	Sim	Não é necessário	Não é necessário	Obrigatório
SMB 3,0	AES-CMAC.	Não	Sim	Não é necessário	Não é necessário	Obrigatório

A Microsoft não recomenda mais o uso `Digitally sign communications (if client agrees)` das configurações de Diretiva de Grupo ou `Digitally sign communications (if server agrees)` . A Microsoft também não recomenda mais o uso das `EnableSecuritySignature` configurações do Registro. Essas opções afetam apenas o comportamento do SMB 1 e podem ser substituídas pela `Digitally sign communications (always)` configuração de Diretiva de Grupo ou pela `RequireSecuritySignature` configuração do Registro. Você também pode obter mais informações do blog da Microsoft.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Fundamentos de assinatura SMB (abrangendo SMB1 e SMB2)]

Impacto na performance da assinatura SMB

Quando as sessões SMB usam a assinatura SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB assinado. A descarga de assinatura SMB é ativada por padrão quando a assinatura SMB está ativada.

O desempenho aprimorado de assinatura SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impactos na performance da assinatura SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A maioria dos clientes do Windows negocia a assinatura SMB por padrão se estiver habilitada no servidor. Se você precisar de proteção SMB para alguns de seus clientes Windows e se a assinatura SMB estiver causando problemas de desempenho, você poderá desativar a assinatura SMB em qualquer um de seus clientes Windows que não precisem de proteção contra ataques de repetição. Para obter informações sobre como desativar a assinatura SMB em clientes Windows, consulte a documentação do Microsoft Windows.

Recomendações para configurar a assinatura SMB

Você pode configurar o comportamento de assinatura SMB entre clientes SMB e o servidor CIFS para atender aos seus requisitos de segurança. As configurações escolhidas ao configurar a assinatura SMB no servidor CIFS dependem de quais são os requisitos de segurança.

Você pode configurar a assinatura SMB no cliente ou no servidor CIFS. Considere as seguintes recomendações ao configurar a assinatura SMB:

Se…	Recomendação…
Você deseja aumentar a segurança da comunicação entre o cliente e o servidor	Torne a assinatura SMB necessária no cliente ativando a `Require Option (Sign always)` configuração de segurança no cliente.
Você deseja que todo o tráfego SMB para uma determinada máquina virtual de storage (SVM) seja assinado	Torne necessária a assinatura SMB no servidor CIFS configurando as configurações de segurança para exigir assinatura SMB.

Consulte a documentação da Microsoft para obter mais informações sobre como configurar as configurações de segurança do cliente Windows.

Diretrizes para assinatura SMB quando vários dados LIFS são configurados

Se você ativar ou desativar a assinatura SMB necessária no servidor SMB, você deve estar ciente das diretrizes para várias configurações LIFS de dados para um SVM.

Quando você configura um servidor SMB, pode haver várias LIFs de dados configuradas. Nesse caso, o

servidor DNS contém várias `A` entradas de Registro para o servidor CIFS, todas usando o mesmo nome de host do servidor SMB, mas cada uma com um endereço IP exclusivo. Por exemplo, um servidor SMB que tem duas LIFs de dados configuradas pode ter as seguintes entradas de Registro DNS `A`:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

O comportamento normal é que, ao alterar a configuração de assinatura SMB necessária, apenas novas conexões de clientes são afetadas pela alteração na configuração de assinatura SMB. No entanto, há uma exceção a esse comportamento. Há um caso em que um cliente tem uma conexão existente com um compartilhamento, e o cliente cria uma nova conexão com o mesmo compartilhamento após a configuração ser alterada, mantendo a conexão original. Nesse caso, tanto a conexão SMB nova quanto a existente adotam os novos requisitos de assinatura SMB.

Considere o seguinte exemplo:

1. Client1 coneta-se a um compartilhamento sem a assinatura SMB necessária usando o caminho `O:\`.
2. O administrador de armazenamento modifica a configuração do servidor SMB para exigir assinatura SMB.
3. O Client1 coneta-se ao mesmo compartilhamento com a assinatura SMB necessária usando o caminho `S:\` (mantendo a conexão usando o caminho `O:\`).
4. O resultado é que a assinatura SMB é usada ao acessar dados `O:\` nas unidades e `S:\` .

Ative ou desative a assinatura SMB necessária para o tráfego SMB de entrada

Você pode impor o requisito para que os clientes assinem mensagens SMB habilitando a assinatura SMB necessária. Se ativado, o ONTAP aceita mensagens SMB somente se elas tiverem assinaturas válidas. Se você quiser permitir a assinatura SMB, mas não a exigir, você pode desativar a assinatura SMB necessária.

Sobre esta tarefa

Por padrão, a assinatura SMB necessária está desativada. Você pode ativar ou desativar a assinatura SMB necessária a qualquer momento.

> A assinatura SMB não está desativada por padrão nas seguintes circunstâncias:
>
> 1. A assinatura SMB necessária está ativada e o cluster é revertido para uma versão do ONTAP que não suporta assinatura SMB.
> 2. O cluster é posteriormente atualizado para uma versão do ONTAP que suporte a assinatura SMB.
>
>   Nestas circunstâncias, a configuração de assinatura SMB que foi originalmente configurada em uma versão suportada do ONTAP é mantida por meio de reversão e atualização subsequente.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de assinatura SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (non-ID-Preserve), a configuração de segurança de assinatura SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se você ativou a assinatura SMB necessária na SVM de origem, habilite manualmente a assinatura SMB necessária no SVM de destino.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a assinatura SMB seja necessária…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Verifique se a assinatura SMB necessária está ativada ou desativada determinando se o valor no `Is Signing Required` campo na saída do comando a seguir está definido para o valor desejado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Exemplo

O exemplo a seguir habilita a assinatura SMB necessária para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Determine se as sessões SMB são assinadas

Você pode exibir informações sobre sessões SMB conetadas no servidor CIFS. Você pode usar essas informações para determinar se as sessões SMB são assinadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as configurações de segurança desejadas.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Todas as sessões assinadas em uma máquina virtual de storage (SVM) especificada	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Detalhes de uma sessão assinada com um Session ID específico no SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Exemplos

O comando a seguir exibe informações de sessão sobre sessões assinadas no SVM VS1. A saída de resumo padrão não exibe o campo de saída "'is Session signed'":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

O comando a seguir exibe informações detalhadas da sessão, incluindo se a sessão está assinada, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Informações relacionadas

Monitoramento de estatísticas de sessão assinadas pelo SMB

Monitorar estatísticas de sessão assinadas pelo SMB

Você pode monitorar estatísticas de sessões SMB e determinar quais sessões estabelecidas são assinadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível de privilégio avançado fornece o `signed_sessions` contador que você pode usar para monitorar o número de sessões SMB assinadas. O `signed_sessions` contador está disponível com os seguintes objetos estatísticos:

- `cifs` Permite monitorar a assinatura SMB para todas as sessões SMB.
- `smb1` Permite monitorar a assinatura SMB para sessões SMB 1,0.
- `smb2` Permite monitorar a assinatura SMB para sessões SMB 2.x e SMB 3,0.

  As estatísticas SMB 3,0 são incluídas na saída para o `smb2` objeto.

Se você quiser comparar o número de sessão assinada com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `signed_sessions` o contador.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra

fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências.

Passos

1. Defina o nível de privilégio como avançado
   `set -privilege advanced`
2. Iniciar uma coleta de dados
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

   Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.
3. Use o `statistics stop` comando para parar de coletar dados para a amostra.
4. Exibir estatísticas de assinatura SMB:

Se você quiser ver informações para…	**Digite…**
Sessões assinadas	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sessões assinadas e sessões estabelecidas
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.
5. Voltar para o nível de privilégio de administrador
   `set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de assinatura SMB 2.x e SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

O comando a seguir interrompe a coleta de dados para a amostra:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

O comando a seguir mostra sessões SMB assinadas e sessões SMB estabelecidas por nó da amostra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

O comando a seguir mostra sessões SMB assinadas para node2 da amostra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

O seguinte comando volta para o nível de privilégio admin:

```
cluster1::*> set -privilege admin
```

Informações relacionadas

Determinar se as sessões SMB são assinadas

"Visão geral do gerenciamento e monitoramento de desempenho"

Configurar a criptografia SMB necessária em servidores SMB para transferências de dados por SMB

Visão geral da criptografia SMB

A encriptação SMB para transferências de dados através de SMB é um melhoramento de segurança que pode ativar ou desativar em servidores SMB. Você também pode configurar a configuração de criptografia SMB desejada em uma base de compartilhamento por compartilhamento por meio de uma configuração de propriedade de compartilhamento.

Por padrão, quando você cria um servidor SMB na máquina virtual de storage (SVM), a criptografia SMB é desativada. Você deve habilitá-lo para aproveitar a segurança aprimorada fornecida pela criptografia SMB.

Para criar uma sessão SMB encriptada, o cliente SMB tem de suportar a encriptação SMB. Os clientes Windows que começam com o Windows Server 2012 e o Windows 8 suportam a encriptação SMB.

A criptografia SMB no SVM é controlada por meio de duas configurações:

- Uma opção de segurança de servidor SMB que habilita a funcionalidade no SVM
- Uma propriedade de compartilhamento SMB que configura a configuração de criptografia SMB em uma base de compartilhamento por compartilhamento

Você pode decidir se deseja exigir criptografia para acesso a todos os dados no SVM ou se exige que a criptografia SMB acesse dados somente em compartilhamentos selecionados. As configurações de nível SVM substituem as configurações de nível de compartilhamento.

A configuração eficaz de criptografia SMB depende da combinação das duas configurações e é descrita na tabela a seguir:

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Verdadeiro	Falso	A criptografia no nível do servidor está habilitada para todos os compartilhamentos na SVM. Com essa configuração, a criptografia acontece para toda a sessão SMB.
Verdadeiro	Verdadeiro	A criptografia no nível do servidor é ativada para todos os compartilhamentos no SVM, independentemente da criptografia no nível de compartilhamento. Com essa configuração, a criptografia acontece para toda a sessão SMB.

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Falso	Verdadeiro	A criptografia no nível de compartilhamento está ativada para compartilhamentos específicos. Com essa configuração, a criptografia acontece a partir da conexão em árvore.
Falso	Falso	Nenhuma criptografia está ativada.

Os clientes SMB que não suportam encriptação não podem estabelecer ligação a um servidor SMB ou partilha que requeira encriptação.

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Impacto na performance da criptografia SMB

Quando as sessões SMB usam criptografia SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB criptografado. A descarga de criptografia SMB é ativada por padrão quando a criptografia SMB está ativada.

O desempenho aprimorado da criptografia SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impacto na performance da criptografia SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A encriptação SMB está desativada por predefinição no servidor SMB. Você deve habilitar a criptografia SMB somente nos compartilhamentos SMB ou servidores SMB que exigem criptografia. Com a criptografia SMB, o ONTAP realiza processamento adicional de descriptografar as solicitações e criptografar as respostas para cada solicitação. A criptografia SMB deve, portanto, ser ativada somente quando necessário.

Ative ou desative a encriptação SMB necessária para o tráfego SMB de entrada

Se pretender exigir encriptação SMB para o tráfego SMB de entrada, pode ativá-la no servidor CIFS ou no nível de partilha. Por padrão, a criptografia SMB não é necessária.

Sobre esta tarefa

Você pode ativar a criptografia SMB no servidor CIFS, que se aplica a todos os compartilhamentos no servidor CIFS. Se não pretender a encriptação SMB necessária para todos os partilhas no servidor CIFS ou se pretender ativar a encriptação SMB necessária para o tráfego SMB de entrada numa base de partilha por partilha, pode desativar a encriptação SMB necessária no servidor CIFS.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de criptografia SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (não-ID-Preserve), a configuração de segurança de criptografia SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se tiver ativado a encriptação SMB na SVM de origem, tem de ativar manualmente a encriptação SMB do servidor CIFS no destino.

Passos

1. Execute uma das seguintes ações:

Se pretender que a encriptação SMB necessária para o tráfego SMB de entrada no servidor CIFS seja…	**Digite o comando…**
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Verifique se a criptografia SMB necessária no servidor CIFS está ativada ou desativada conforme desejado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   O `is-smb-encryption-required` campo é exibido `true` se a criptografia SMB necessária estiver ativada no servidor CIFS e `false` se estiver desativada.

Exemplo

O exemplo a seguir habilita a criptografia SMB necessária para o tráfego SMB de entrada para o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Determine se os clientes estão conetados usando sessões SMB criptografadas

Você pode exibir informações sobre sessões SMB conetadas para determinar se os clientes estão usando conexões SMB criptografadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as configurações de segurança desejadas.

Sobre esta tarefa

As sessões de clientes SMB podem ter um dos três níveis de criptografia:

- `unencrypted`

  A sessão SMB não está encriptada. Nem a criptografia no nível de máquina virtual de storage (SVM) nem no nível de compartilhamento são configuradas.

- `partially-encrypted`

  A criptografia é iniciada quando ocorre a conexão em árvore. A criptografia no nível de compartilhamento está configurada. A criptografia no nível da SVM não está ativada.

- `encrypted`

  A sessão SMB está totalmente encriptada. A criptografia no nível da SVM está ativada. A encriptação do nível de partilha pode ou não estar ativada. A configuração de criptografia no nível da SVM substitui a configuração de criptografia no nível de compartilhamento.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Sessões com uma configuração de criptografia especificada para sessões em um SVM especificado	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Se você quiser exibir informações sobre…	Digite o comando…
A configuração de criptografia para um Session ID específico em um SVM especificado	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Exemplos

O comando a seguir exibe informações detalhadas da sessão, incluindo a configuração de criptografia, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Monitorar estatísticas de criptografia SMB

Você pode monitorar estatísticas de criptografia SMB e determinar quais sessões estabelecidas e conexões de compartilhamento são criptografadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível avançado de privilégios fornece os seguintes contadores, que podem ser utilizados para monitorizar o número de sessões SMB encriptadas e partilhar ligações:

Nome do contador	Descrições
`encrypted_sessions`	Fornece o número de sessões criptografadas do SMB 3,0

Nome do contador	Descrições
`encrypted_share_connections`	Fornece o número de compartilhamentos criptografados nos quais uma conexão em árvore aconteceu
`rejected_unencrypted_sessions`	Fornece o número de configurações de sessão rejeitadas devido à falta de capacidade de criptografia do cliente
`rejected_unencrypted_shares`	Fornece o número de mapeamentos de compartilhamento rejeitados devido à falta de capacidade de criptografia do cliente

Esses contadores estão disponíveis com os seguintes objetos estatísticos:

- `cifs` Permite monitorizar a encriptação SMB para todas as sessões SMB 3,0.

  As estatísticas SMB 3,0 são incluídas na saída para o `cifs` objeto. Se você quiser comparar o número de sessões criptografadas com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `encrypted_sessions` o contador.

  Se você quiser comparar o número de conexões de compartilhamento criptografadas com o número total de conexões de compartilhamento, você pode comparar a saída para o contador com a saída `connected_shares` para `encrypted_share_connections` o contador.

- `rejected_unencrypted_sessions` Fornece o número de vezes que uma tentativa foi feita para estabelecer uma sessão SMB que requer criptografia de um cliente que não suporta criptografia SMB.
- `rejected_unencrypted_shares` Fornece o número de vezes que uma tentativa foi feita para se conetar a um compartilhamento SMB que requer criptografia de um cliente que não suporta criptografia SMB.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências.

Passos

1. Defina o nível de privilégio como avançado
   `set -privilege advanced`
2. Iniciar uma coleta de dados
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

   Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.

3. Use o `statistics stop` comando para parar de coletar dados para a amostra.
4. Exibir estatísticas de criptografia SMB:

Se você quiser ver informações para…	Digite…
Sessões criptografadas	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sessões criptografadas e sessões estabelecidas
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Conexões de compartilhamento criptografadas
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Conexões de compartilhamento criptografadas e compartilhamentos conetados	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sessões não criptografadas rejeitadas	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Conexões de compartilhamento não criptografadas rejeitadas
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.

5. Voltar para o nível de privilégio de administrador
`set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de criptografia SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

O comando a seguir interrompe a coleta de dados para essa amostra:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

O comando a seguir mostra sessões criptografadas SMB e sessões estabelecidas SMB pelo nó da amostra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

O comando a seguir mostra o número de sessões SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

O comando a seguir mostra o número de compartilhamentos SMB conetados e compartilhamentos SMB criptografados pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

O comando a seguir mostra o número de conexões de compartilhamento SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Informações relacionadas

Determinando quais objetos e contadores de estatísticas estão disponíveis

"Visão geral do gerenciamento e monitoramento de desempenho"

Comunicação de sessão LDAP segura

Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você

deve configurar as configurações de segurança do servidor CIFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`.

A assinatura LDAP e a vedação no tráfego CIFS são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Ative a assinatura LDAP e a vedação no servidor CIFS

Antes que o servidor CIFS possa usar assinatura e vedação para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor CIFS para habilitar a assinatura e a vedação LDAP.

Antes de começar

Você deve consultar o administrador do servidor AD para determinar os valores de configuração de segurança apropriados.

Passos

1. Configure a configuração de segurança do servidor CIFS que permite o tráfego assinado e selado com servidores LDAP do ative Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

2. Verifique se a configuração de segurança de assinatura e vedação LDAP está definida corretamente: `vserver cifs security show -vserver` *`vserver_name`*

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX, como usuários, grupos e netgroups, você deverá ativar a configuração correspondente com `-session-security` a opção do `vserver services name-service ldap client modify` comando.

Configurar LDAP em TLS

Exporte uma cópia do certificado de CA raiz autoassinado

Para usar LDAP em SSL/TLS para proteger a comunicação do ative Directory, primeiro você deve exportar uma cópia do certificado CA raiz autoassinado do ative Directory Service para um arquivo de certificado e convertê-lo em um arquivo de texto ASCII. Esse arquivo de texto é usado pelo ONTAP para instalar o certificado na máquina virtual de storage (SVM).

Antes de começar

O Serviço de certificados do ative Directory já deve estar instalado e configurado para o domínio ao qual o servidor CIFS pertence. Você pode encontrar informações sobre a instalação e configuração dos Serviços de

certificados do ative diretor consultando a Biblioteca Microsoft TechNet.

"Microsoft TechNet Library: technet.microsoft.com"

Passo

1. Obtenha um certificado de CA raiz do controlador de domínio que está no `.pem` formato de texto.

   "Microsoft TechNet Library: technet.microsoft.com"

Depois de terminar

Instale o certificado no SVM.

Informações relacionadas

"Microsoft TechNet Library"

Instale o certificado de CA raiz autoassinado no SVM

Se a autenticação LDAP com TLS for necessária ao vincular a servidores LDAP, primeiro você deverá instalar o certificado de CA raiz autoassinado no SVM.

Sobre esta tarefa

Quando o LDAP sobre TLS está ativado, o cliente LDAP do ONTAP no SVM não oferece suporte a certificados revogados no ONTAP 9.0 e 9,1.

A partir do ONTAP 9.2, todos os aplicativos do ONTAP que usam comunicações TLS podem verificar o status do certificado digital usando o protocolo OCSP (Online Certificate Status Protocol). Se o OCSP estiver ativado para LDAP através de TLS, os certificados revogados serão rejeitados e a conexão falhará.

Passos

1. Instale o certificado CA raiz autoassinado:
   a. Inicie a instalação do certificado: `security certificate install -vserver vserver_name -type server-ca`

      A saída do console exibe a seguinte mensagem: `Please enter Certificate: Press <Enter> when done`

   b. Abra o arquivo de certificado `.pem` com um editor de texto, copie o certificado, incluindo as linhas que começam com `-----BEGIN CERTIFICATE-----` e terminam com `-----END CERTIFICATE-----`, e cole o certificado após o prompt de comando.
   c. Verifique se o certificado é exibido corretamente.
   d. Conclua a instalação pressionando Enter.
2. Verifique se o certificado está instalado: `security certificate show -vserver *vserver_name*`

Ative LDAP através de TLS no servidor

Antes que o servidor SMB possa usar TLS para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor SMB para ativar o LDAP sobre TLS.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative

Directory (AD) e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores AD, use o `-try-channel-binding-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.

Para saber mais, consulte:

- "Visão geral da LDAP"
- "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows".

Passos

1. Configure a configuração de segurança do servidor SMB que permite a comunicação LDAP segura com servidores LDAP do ative Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Verifique se a configuração de segurança LDAP sobre TLS está definida como `true`: `vserver cifs security show -vserver vserver_name`

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX (como usuários, grupos e netgroups), você também deve modificar a `-use-start-tls` opção usando o `vserver services name-service ldap client modify` comando.

Configure o SMB Multichannel para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

  O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

  O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilégio avançado):

- `-max-connections-per-session`

O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

  O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Ative SMB Multichannel no servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

```
vserver cifs session show
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
       Workstation IP Address: 10.1.1.1
      Authentication Mechanism: NTLMv1
         User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Configure o usuário padrão do Windows para mapeamentos de usuários UNIX no servidor SMB

Configure o usuário UNIX padrão

Você pode configurar o usuário UNIX padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar o usuário UNIX padrão.

Sobre esta tarefa

Por padrão, o nome do usuário UNIX padrão é "'pcuser'", o que significa que, por padrão, o mapeamento de usuário para o usuário UNIX padrão está habilitado. Você pode especificar outro nome para usar como usuário UNIX padrão. O nome especificado deve existir nos bancos de dados do serviço de nomes configurados para a máquina virtual de storage (SVM). Se essa opção for definida como uma cadeia de carateres nula, ninguém poderá acessar o servidor CIFS como um usuário padrão UNIX. Ou seja, cada usuário deve ter uma conta no banco de dados de senhas antes de poder acessar o servidor CIFS.

Para que um usuário se conete ao servidor CIFS usando a conta de usuário UNIX padrão, o usuário deve atender aos seguintes pré-requisitos:

- O utilizador está autenticado.
- O usuário está no banco de dados de usuários do Windows local do servidor CIFS, no domínio doméstico do servidor CIFS ou em um domínio confiável (se pesquisas de mapeamento de nomes de vários domínios estiverem ativadas no servidor CIFS).
- O nome de usuário não é explicitamente mapeado para uma cadeia de carateres nula.

Passos

1. Configure o usuário UNIX padrão:

Se você quiser …	Introduza …
Use o usuário padrão do UNIX "'pcuser'"	`vserver cifs options modify -default -unix-user pcuser`
Use outra conta de usuário UNIX como usuário padrão	`vserver cifs options modify -default -unix-user` *`user_name`*
Desative o usuário UNIX padrão	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verifique se o usuário UNIX padrão está configurado corretamente: `vserver cifs options show -vserver` *`vserver_name`*

   No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "'pcuser'":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure o usuário UNIX convidado

Configurar a opção de usuário UNIX convidado significa que os usuários que fazem login de domínios não confiáveis são mapeados para o usuário UNIX convidado e podem se conetar ao servidor CIFS. Alternativamente, se você quiser que a autenticação de usuários de domínios não confiáveis falhe, você não deve configurar o usuário UNIX convidado. O padrão é não permitir que usuários de domínios não confiáveis se conetem ao servidor CIFS (a conta UNIX convidada não está configurada).

Sobre esta tarefa

Você deve ter em mente o seguinte ao configurar a conta UNIX Guest:

- Se o servidor CIFS não puder autenticar o usuário em um controlador de domínio para o domínio doméstico ou um domínio confiável ou o banco de dados local e essa opção estiver ativada, o servidor CIFS considera o usuário como um usuário convidado e mapeia o usuário para o usuário UNIX especificado.
- Se essa opção for definida como uma cadeia de carateres nula, o usuário UNIX convidado será desativado.
- Você deve criar um usuário UNIX para usar como usuário UNIX convidado em um dos bancos de dados do serviço de nomes de máquina virtual de armazenamento (SVM).
- Um usuário conetado como um usuário convidado é automaticamente membro do grupo BUILTIN/convidados no servidor CIFS.
- A opção 'homedirs-public' aplica-se apenas a utilizadores autenticados. Um usuário conetado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite…
Configure o usuário UNIX convidado	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Desative o usuário UNIX convidado	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verifique se o usuário UNIX convidado está configurado corretamente: `vserver cifs options show -vserver vserver_name`

   No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "'pcuser'":

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

Mapeie o grupo administrators para root

Se você tiver apenas clientes CIFS em seu ambiente e sua máquina virtual de storage (SVM) tiver sido configurada como um sistema de storage multiprotocolo, você deverá ter pelo menos uma conta do Windows que tenha privilégios de raiz para acessar arquivos no SVM; caso contrário, não será possível gerenciar o SVM porque não tem direitos de usuário suficientes.

Sobre esta tarefa

No entanto, se o sistema de armazenamento tiver sido configurado apenas para NTFS, o `/etc` diretório tem uma ACL no nível do ficheiro que permite ao grupo de administradores aceder aos ficheiros de configuração do ONTAP.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a opção de servidor CIFS que mapeia o grupo de administradores para fazer root conforme apropriado:

Se você quiser…	Então…
Mapeie os membros do grupo de administradores para fazer root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Todas as contas do grupo administrators são consideradas root, mesmo que você não tenha uma `/etc/usermap.cfg` entrada mapeando as contas para root. Se você criar um arquivo usando uma conta que pertence ao grupo administrators, o arquivo será de propriedade do root quando você exibir o arquivo de um cliente UNIX.
Desative o mapeamento dos membros do grupo de administradores para fazer root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` As contas no grupo administrators não são mais mapeadas para o root. Você só pode mapear explicitamente um único usuário para o root.

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exiba informações sobre quais tipos de usuários estão conetados em sessões SMB

Você pode exibir informações sobre que tipo de usuários estão conetados em sessões SMB. Isso pode ajudar você a garantir que apenas o tipo apropriado de usuário esteja se conetando por sessões SMB na máquina virtual de storage (SVM).

Sobre esta tarefa

Os seguintes tipos de usuários podem se conetar através de sessões SMB:

- `local-user`

  Autenticado como um usuário CIFS local

- `domain-user`

  Autenticado como um usuário de domínio (do domínio doméstico do servidor CIFS ou de um domínio confiável)

- `guest-user`

  Autenticado como usuário convidado

- `anonymous-user`

  Autenticado como um usuário anônimo ou nulo

Passos

1. Determine que tipo de usuário está conetado em uma sessão SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Se você quiser exibir informações de tipo de usuário para sessões estabelecidas…	Digite o seguinte comando…
Para todas as sessões com um tipo de usuário especificado	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Para um usuário específico

Exemplos

O comando a seguir exibe informações de sessão sobre o tipo de usuário para sessões no SVM VS1 estabelecido pelo usuário "" iebubs user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Opções de comando para limitar o consumo excessivo de recursos do cliente Windows

As opções para o `vserver cifs options modify` comando permitem controlar o consumo de recursos para clientes Windows. Isso pode ser útil se algum cliente estiver fora dos limites normais de consumo de recursos, por exemplo, se houver um número excepcionalmente alto de arquivos abertos, sessões abertas ou solicitações Change Notify.

As seguintes opções para o `vserver cifs options modify` comando foram adicionadas para controlar o consumo de recursos do cliente Windows. Se o valor máximo de qualquer uma dessas opções for excedido, a solicitação será negada e uma mensagem EMS será enviada. Uma mensagem de aviso EMS também é enviada quando 80% do limite configurado para essas opções é atingido.

- `-max-opens-same-file-per-tree`

  Número máximo de aberturas no mesmo arquivo por árvore CIFS

- `-max-same-user-sessions-per-connection`

  Número máximo de sessões abertas pelo mesmo usuário por conexão

- `-max-same-tree-connect-per-session`

  O número máximo de árvores se coneta no mesmo compartilhamento por sessão

- `-max-watches-set-per-tree`

  Número máximo de relógios (também conhecido como *change notifica*) estabelecido por árvore

Consulte as páginas man para ver os limites padrão e para exibir a configuração atual.

A partir do ONTAP 9.4, os servidores que executam o SMB versão 2 ou posterior podem limitar o número de solicitações pendentes (*créditos SMB*) que o cliente pode enviar para o servidor em uma conexão SMB. O gerenciamento de créditos SMB é iniciado pelo cliente e controlado pelo servidor.

O número máximo de solicitações pendentes que podem ser concedidas em uma conexão SMB é controlado pela `-max-credits` opção. O valor padrão para essa opção é 128.

Melhore o desempenho do cliente com os oplocks tradicionais e de leasing

Melhore o desempenho do cliente com a visão geral tradicional e dos oplocks de leasing

Os oplocks tradicionais (bloqueios oportunistas) e os oplocks de leasing permitem que um cliente SMB em determinados cenários de compartilhamento de arquivos execute o armazenamento em cache do lado do cliente de informações de leitura antecipada, gravação e bloqueio. Um cliente pode então ler ou gravar em um arquivo sem lembrar regularmente o servidor de que precisa de acesso ao arquivo em questão. Isso melhora o desempenho reduzindo o tráfego de rede.

Os calços de leasing são uma forma melhorada de oplocks disponíveis com o protocolo SMB 2,1 e posterior. Os locks permitem que um cliente obtenha e preserve o estado de cache do cliente em várias aberturas SMB originadas de si mesmo.

Os calços podem ser controlados de duas maneiras:

- Por uma propriedade share, usando o `vserver cifs share create` comando quando o compartilhamento é criado, ou o `vserver share properties` comando após a criação.
- Por uma propriedade de qtree, usando o `volume qtree create` comando quando a qtree é criada, ou os `volume qtree oplock` comandos após a criação.

Escreva considerações sobre perda de dados de cache ao usar os oplocks

Em algumas circunstâncias, se um processo tem um oplock exclusivo em um arquivo e um segundo processo tenta abrir o arquivo, o primeiro processo deve invalidar dados em cache e flush escreve e bloqueia. O cliente deve então abandonar o oplock e o acesso ao arquivo. Se houver uma falha de rede durante esse flush, os dados de gravação em cache podem ser perdidos.

- Possibilidades de perda de dados

  Qualquer aplicativo que tenha dados gravados em cache pode perder esses dados sob o seguinte conjunto de circunstâncias:

- A conexão é feita usando SMB 1,0.
- Tem um oplock exclusivo no arquivo.
- É dito para interromper esse oplock ou fechar o arquivo.
- Durante o processo de limpeza do cache de gravação, a rede ou o sistema de destino gera um erro.

- Erro de manipulação e conclusão de gravação

  O cache em si não tem nenhum tratamento de erros - os aplicativos fazem.quando o aplicativo faz uma gravação no cache, a gravação é sempre concluída. Se o cache, por sua vez, faz uma gravação no sistema de destino em uma rede, ele deve assumir que a gravação é concluída porque, se não fizer, os dados são perdidos.

Ative ou desative os oplocks ao criar compartilhamentos SMB

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Os Oplocks são ativados em compartilhamentos SMB residentes em máquinas virtuais de armazenamento (SVMs). Em algumas circunstâncias, você pode querer desativar os oplocks. Você pode ativar ou desativar os oplocks em uma base de compartilhamento por compartilhamento.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a configuração de volume de oplock A desativação de oplocks na partilha desativa os oplocks oportunistas e de leasing.

Você pode especificar outras propriedades de compartilhamento além de especificar a propriedade de compartilhamento de oplock usando uma lista delimitada por vírgulas. Você também pode especificar outros parâmetros de compartilhamento.

Passos

1. Execute a ação aplicável:

Se você quiser…	Então…
Ative os oplocks em um compartilhamento durante a criação de compartilhamento	Introduza o seguinte comando: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Se desejar que o compartilhamento tenha apenas as propriedades padrão de compartilhamento, que são `oplocks`, `browsable` e `changenotify` ativadas, não será necessário especificar o `-share -properties` parâmetro ao criar um compartilhamento SMB. Se você quiser qualquer combinação de propriedades de compartilhamento diferente do padrão, especifique o `-share-properties` parâmetro com a lista de propriedades de compartilhamento a ser usada para esse compartilhamento.
Desative os oplocks em um compartilhamento durante a criação de compartilhamento	Introduza o seguinte comando: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Ao desativar os oplocks, você deve especificar uma lista de propriedades de compartilhamento ao criar o compartilhamento, mas não deve especificar a `oplocks` propriedade.

Informações relacionadas

Ativar ou desativar os oplocks em compartilhamentos SMB existentes

Monitorização do estado de oplock

Comandos para ativar ou desativar oplocks em volumes e qtrees

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Você precisa saber os comandos para ativar ou desativar os oplocks em volumes ou qtrees. Você também deve saber quando você pode ativar ou desativar os oplocks em volumes e qtrees.

- Os calços são ativados em volumes por predefinição.
- Não é possível desativar os oplocks ao criar um volume.
- Você pode ativar ou desativar os oplocks em volumes existentes para SVMs a qualquer momento.
- Você pode ativar os oplocks em qtrees para SVMs.

  A configuração do modo de oplock é uma propriedade da ID de qtree 0, a qtree padrão que todos os volumes têm. Se você não especificar uma configuração de oplock ao criar uma qtree, a qtree herdará a configuração de oplock do volume pai, que é habilitada por padrão. No entanto, se você especificar uma configuração de oplock na nova qtree, ela terá precedência sobre a configuração de oplock no volume.

Se você quiser…	Use este comando…
Ative os oplocks em volumes ou qtrees	`volume qtree oplocks` com o `-oplock-mode` parâmetro definido como `enable`
Desative os oplocks em volumes ou qtrees	`volume qtree oplocks` com o `-oplock-mode` parâmetro definido como `disable`

Informações relacionadas

Monitorização do estado de oplock

Ative ou desative os oplocks em compartilhamentos SMB existentes

Os Oplocks são ativados em compartilhamentos SMB em máquinas virtuais de armazenamento (SVMs) por padrão. Em algumas circunstâncias, você pode querer desativar os oplocks; alternativamente, se você tiver desabilitado previamente os oplocks em uma ação, você pode querer reativar os oplocks.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a ativação de oplocks no volume. Desativar os oplocks na partilha, desativa os oplocks oportunistas e de leasing. Você pode ativar ou desativar os oplocks em compartilhamentos existentes a qualquer momento.

Passo

1. Execute a ação aplicável:

Se você quiser…	Então…
Ative os oplocks em um compartilhamento modificando um compartilhamento existente	Introduza o seguinte comando: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` Você pode especificar propriedades de compartilhamento adicionais a serem adicionadas usando uma lista delimitada por vírgulas. As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento. Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.
Desative os oplocks em um compartilhamento modificando um compartilhamento existente	Introduza o seguinte comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` Você pode especificar propriedades de compartilhamento adicionais para remover usando uma lista delimitada por vírgulas. As propriedades de compartilhamento que você remover são excluídas da lista existente de propriedades de compartilhamento; no entanto, as propriedades de compartilhamento configuradas anteriormente que você não remove permanecem em vigor.

Exemplos

O comando a seguir habilita os oplocks para o compartilhamento chamado "Engenharia" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

O comando a seguir desativa os oplocks para a ação chamada "Engenharia" no SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Informações relacionadas

Ativar ou desativar os oplocks ao criar compartilhamentos SMB

Monitorização do estado de oplock

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Monitorar o status de oplock

Você pode monitorar e exibir informações sobre o status de oplock Você pode usar essas informações para determinar quais arquivos têm oplocks, quais são o nível de oplock e o nível de estado de oplock e se o leasing de oplock é usado. Você também pode determinar informações sobre bloqueios que você pode precisar quebrar manualmente.

Sobre esta tarefa

Você pode exibir informações sobre todos os oplocks em forma de resumo ou em um formulário de lista detalhado. Você também pode usar parâmetros opcionais para exibir informações sobre um subconjunto menor de bloqueios existentes. Por exemplo, você pode especificar que a saída retorna apenas bloqueia com o endereço IP do cliente especificado ou com o caminho especificado.

Você pode exibir as seguintes informações sobre os oplocks tradicionais e de leasing:

- SVM, nó, volume e LIF em que o oplock
- Bloquear UUID
- Endereço IP do cliente com o oplock
- Caminho no qual o oplock é estabelecido
- Protocolo de bloqueio (SMB) e tipo (oplock)
- Estado de bloqueio
- Nível do calço
- Estado da conexão e tempo de expiração do SMB
- Abra o ID do grupo se for concedida uma locação de oplock

Consulte a `vserver oplocks show` página de manual para obter uma descrição detalhada de cada parâmetro.

Passos

1. Apresentar o estado de oplock utilizando o `vserver locks show` comando.

Exemplos

O comando a seguir exibe informações padrão sobre todos os bloqueios. O oplock no ficheiro apresentado é concedido com um `read-batch` nível de oplock:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

O exemplo a seguir exibe informações mais detalhadas sobre o bloqueio em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um leasing de oplock é concedido no arquivo com um `batch` nível de oplock a um cliente com um endereço IP de `10.3.1.3`:

> Ao exibir informações detalhadas, o comando fornece saída separada para informações de oplock e sharelock. Este exemplo mostra apenas a saída da secção de oplock

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Informações relacionadas

Ativar ou desativar os oplocks ao criar compartilhamentos SMB

Ativar ou desativar os oplocks em compartilhamentos SMB existentes

Comandos para ativar ou desativar oplocks em volumes e qtrees

Aplique objetos de Diretiva de Grupo a servidores SMB

Aplicar objetos de Diretiva de Grupo à visão geral dos servidores SMB

Seu servidor SMB oferece suporte a objetos de Diretiva de Grupo (GPOs), um conjunto de regras conhecidas como *atributos de diretiva de grupo* que se aplicam a computadores em um ambiente do ative Directory. Você pode usar GPOs para gerenciar centralmente as configurações de todas as máquinas virtuais de storage (SVMs) no cluster que pertence ao mesmo domínio do ative Directory.

Quando os GPOs estão ativados no servidor SMB, o ONTAP envia consultas LDAP ao servidor do ative Directory solicitando informações de GPO. Se houver definições de GPO aplicáveis ao servidor SMB, o

servidor do ative Directory retornará as seguintes informações de GPO:

- Nome GPO
- Versão GPO atual
- Localização da definição GPO
- Listas de UUIDs (identificadores universalmente exclusivos) para conjuntos de políticas GPO

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

"Auditoria de SMB e NFS e rastreamento de segurança"

GPOs compatíveis

Embora nem todos os objetos de Diretiva de Grupo (GPOs) sejam aplicáveis às máquinas virtuais de storage (SVMs) habilitadas para CIFS, os SVMs podem reconhecer e processar o conjunto relevante de GPOs.

Os GPOs a seguir são compatíveis atualmente com SVMs:

- Definições avançadas de configuração da política de auditoria:

  Acesso a objetos: Preparação da Política de Acesso Central

  Especifica o tipo de eventos a serem auditados para o estadiamento da política de acesso central (CAP), incluindo as seguintes configurações:

  - Não faça auditoria
  - Audite apenas eventos de sucesso
  - Auditar apenas eventos de falha
  - Audite eventos de sucesso e falha

  > Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

  Defina utilizando a `Audit Central Access Policy Staging` definição no `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Para usar configurações avançadas de GPO de diretiva de auditoria, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições do registo:

  - Intervalo de atualização da política de grupo para SVM habilitado para CIFS

    Defina utilizando o `Registry` GPO.

- Atualizar desvio aleatório da política de grupo

  Defina utilizando o `Registry` GPO.

- Publicação hash para BranchCache

  A publicação Hash para o GPO BranchCache corresponde ao modo de operação BranchCache. Os três modos de operação suportados a seguir são suportados:

  - Por compartilhamento
  - Todos os compartilhamentos
  - Desativado definido utilizando o `Registry` GPO.

- Suporte à versão hash para BranchCache

  As seguintes três configurações de versão hash são suportadas:

  - BranchCache versão 1
  - BranchCache versão 2
  - BranchCache versões 1 e 2 definidas usando o `Registry` GPO.

> Para usar as configurações de GPO do BranchCache, o BranchCache deve ser configurado no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se o BranchCache não estiver configurado no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições de segurança
  - Política de auditoria e log de eventos
    - Audite eventos de logon

      Especifica o tipo de eventos de logon a serem auditados, incluindo as seguintes configurações:

      - Não faça auditoria
      - Audite apenas eventos de sucesso
      - Auditoria em eventos de falha
      - Audite eventos de sucesso e falha definidos usando a `Audit logon events` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

    - Auditar o acesso a objeto

      Especifica o tipo de acesso a objeto a ser auditado, incluindo as seguintes configurações:

      - Não faça auditoria
      - Audite apenas eventos de sucesso
      - Auditoria em eventos de falha

- Audite eventos de sucesso e falha definidos usando a `Audit object access` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Método de retenção de log

  Especifica o método de retenção do log de auditoria, incluindo as seguintes configurações:

  - Substituir o registo de eventos quando o tamanho do ficheiro de registo exceder o tamanho máximo do registo
  - Não substituir o registo de eventos (limpar registo manualmente) definido utilizando a `Retention method for security log` definição no `Event Log` GPO.

- Tamanho máximo do registo

  Especifica o tamanho máximo do log de auditoria.

  Defina utilizando a `Maximum security log size` definição no `Event Log` GPO.

> Para usar a diretiva de auditoria e as configurações de GPO de log de eventos, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

◦ Segurança do sistema de arquivos

Especifica uma lista de arquivos ou diretórios nos quais a segurança de arquivos é aplicada por meio de um GPO.

Defina utilizando o `File System` GPO.

> O caminho do volume para o qual o GPO de segurança do sistema de arquivos está configurado deve existir na SVM.

◦ Política Kerberos

- Inclinação máxima do relógio

  Especifica a tolerância máxima em minutos para a sincronização do relógio do computador.

  Defina utilizando a `Maximum tolerance for computer clock synchronization` definição no `Account Policies/Kerberos Policy` GPO.

- Idade máxima do bilhete

  Especifica a vida útil máxima em horas para o ticket de usuário.

  Defina utilizando a `Maximum lifetime for user ticket` definição no `Account Policies/Kerberos Policy` GPO.

- Idade máxima de renovação do bilhete

  Especifica o tempo de vida máximo em dias para a renovação do ticket do usuário.

Defina utilizando a `Maximum lifetime for user ticket renewal` definição no `Account Policies/Kerberos Policy` GPO.

- Atribuição de direitos de utilizador (direitos de privilégio)
  - Assuma a propriedade

    Especifica a lista de usuários e grupos que têm o direito de assumir a propriedade de qualquer objeto que possa ser protegido.

    Defina utilizando a `Take ownership of files or other objects` definição no `Local Policies/User Rights Assignment` GPO.

  - Privilégio de segurança

    Especifica a lista de usuários e grupos que podem especificar opções de auditoria para acesso a objetos de recursos individuais, como arquivos, pastas e objetos do ative Directory.

    Defina utilizando a `Manage auditing and security log` definição no `Local Policies/User Rights Assignment` GPO.

  - Privilégio Change Notify (verificação de desvio transversal)

    Especifica a lista de usuários e grupos que podem atravessar árvores de diretório, mesmo que os usuários e grupos possam não ter permissões no diretório atravessado.

O mesmo privilégio é necessário para que os usuários recebam notificações de alterações em arquivos e diretórios. Defina utilizando a `Bypass traverse checking` definição no `Local Policies/User Rights Assignment` GPO.

- Valores do registo
  - Definição de assinatura necessária

    Especifica se a assinatura SMB necessária está ativada ou desativada.

Defina utilizando a `Microsoft network server: Digitally sign communications (always)` definição no `Security Options` GPO.

- Restringir o anonimato

Especifica quais são as restrições para usuários anônimos e inclui as seguintes três configurações de GPO:

- Sem enumeração de contas SAM (Security Account Manager):

  Esta configuração de segurança determina quais permissões adicionais são concedidas para conexões anônimas ao computador. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM`

`accounts` definição no `Local Policies/Security Options` GPO.

- Nenhuma enumeração de contas e compartilhamentos SAM

  Esta configuração de segurança determina se a enumeração anônima de contas e compartilhamentos SAM é permitida. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM accounts and shares` definição no `Local Policies/Security Options` GPO.

- Restringir o acesso anônimo a compartilhamentos e pipes nomeados

  Essa configuração de segurança restringe o acesso anônimo a compartilhamentos e pipes. Esta opção é apresentada como `no-access` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Restrict anonymous access to Named Pipes and Shares` definição no `Local Policies/Security Options` GPO.

  Ao exibir informações sobre políticas de grupo definidas e aplicadas, o `Resultant restriction for anonymous user` campo de saída fornece informações sobre a restrição resultante das três configurações de GPO anônimo restrito. As possíveis restrições resultantes são as seguintes:

° `no-access`

O usuário anônimo tem acesso negado aos compartilhamentos especificados e pipes nomeados e não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se o `Network access: Restrict anonymous access to Named Pipes and Shares` GPO estiver ativado.

° `no-enumeration`

O usuário anônimo tem acesso aos compartilhamentos especificados e pipes nomeados, mas não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O ou os `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs estão ativados.

° `no-restriction`

O usuário anônimo tem acesso total e pode usar enumeração. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`Os GPOs e `Network access: Do not allow anonymous enumeration of SAM accounts and shares` os GPOs estão desativados.

- Grupos restritos

  Você pode configurar grupos restritos para gerenciar centralmente a associação de grupos internos ou definidos pelo usuário. Quando você aplica um grupo restrito por meio de uma política de grupo, a associação de um grupo local de servidor CIFS é definida automaticamente para corresponder às configurações da lista de membros definidas na política de grupo aplicada.

  Defina utilizando o `Restricted Groups` GPO.

- Definições da política de acesso central

  Especifica uma lista de políticas de acesso central. As políticas de acesso central e as regras de política de acesso central associadas determinam permissões de acesso para vários arquivos no SVM.

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

"Auditoria de SMB e NFS e rastreamento de segurança"

Modificação das configurações de segurança Kerberos do servidor CIFS

Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

Utilizar a assinatura SMB para melhorar a segurança da rede

Configuração da verificação transversal de derivação

Configurando restrições de acesso para usuários anônimos

Requisitos para usar GPOs com seu servidor SMB

Para usar objetos de diretiva de grupo (GPOs) com seu servidor SMB, o sistema deve atender a vários requisitos.

- O SMB deve ser licenciado no cluster. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.
- Um servidor SMB deve ser configurado e Unido a um domínio do ative Directory do Windows.
- O status de administrador do servidor SMB deve estar ativado.
- Os GPOs devem ser configurados e aplicados à Unidade organizacional do ative Directory (ou) do Windows que contém o objeto de computador servidor SMB.
- O suporte ao GPO deve estar ativado no servidor SMB.

Ative ou desative o suporte de GPO em um servidor CIFS

Você pode ativar ou desativar o suporte de GPO (Group Policy Object) em um servidor CIFS. Se você habilitar o suporte a GPO em um servidor CIFS, os GPOs aplicáveis definidos na diretiva de grupo - a diretiva aplicada à unidade organizacional (ou) que contém o objeto computador servidor CIFS - serão aplicados ao servidor CIFS.

Sobre esta tarefa

Os GPOs não podem ser ativados em servidores CIFS no modo de grupo de trabalho.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
Desativar GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status disabled`

2. Verifique se o suporte GPO está no estado desejado: `vserver cifs group-policy show -vserver +vserver_name_`

   O status da Diretiva de Grupo para servidores CIFS no modo de grupo de trabalho é exibido como "habilitado".

Exemplo

O exemplo a seguir habilita o suporte a GPO na máquina virtual de storage (SVM) VS1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Informações relacionadas

GPOs compatíveis

Requisitos para usar GPOs com seu servidor CIFS

Como os GPOs são atualizados no servidor CIFS

Atualizar manualmente as definições de GPO no servidor CIFS

Exibindo informações sobre as configurações do GPO

Como os GPOs são atualizados no servidor SMB

Como os GPOs são atualizados na visão geral do servidor CIFS

Por padrão, o ONTAP recupera e aplica alterações de Objeto de Diretiva de Grupo (GPO) a cada 90 minutos. As configurações de segurança são atualizadas a cada 16 horas. Se você quiser atualizar os GPOs para aplicar novas configurações de política de

GPO antes que o ONTAP as atualize automaticamente, você pode acionar uma atualização manual em um servidor CIFS com um comando ONTAP.

- Por padrão, todos os GPOs são verificados e atualizados conforme necessário a cada 90 minutos.

  Este intervalo é configurável e pode ser definido utilizando as `Refresh interval` definições e `Random offset` GPO.

  O ONTAP consulta o ative Directory quanto a alterações nos GPOs. Se os números de versão do GPO registrados no ative Directory forem maiores do que os do servidor CIFS, o ONTAP recuperará e aplicará os novos GPOs. Se os números de versão forem os mesmos, os GPOs no servidor CIFS não serão atualizados.

- Os GPOs são atualizados a cada 16 horas.

  O ONTAP recupera e aplica GPOs de configurações de segurança a cada 16 horas, independentemente de estes GPOs terem sido alterados ou não.

  > O valor padrão de 16 horas não pode ser alterado na versão atual do ONTAP. É uma configuração padrão do cliente Windows.

- Todos os GPOs podem ser atualizados manualmente com um comando ONTAP.

  Este comando simula o comando Windows `gpupdate.exe`/force.

Informações relacionadas

Atualizar manualmente as definições de GPO no servidor CIFS

Atualizar manualmente as definições de GPO no servidor CIFS

Se pretender atualizar imediatamente as definições do GPO (Group Policy Object) no servidor CIFS, pode atualizar manualmente as definições. Você pode atualizar apenas as configurações alteradas ou forçar uma atualização para todas as configurações, incluindo as configurações que foram aplicadas anteriormente, mas não foram alteradas.

Passo

1. Execute a ação apropriada:

Se você quiser atualizar…	Digite o comando…
Definições GPO alteradas	`vserver cifs group-policy update -vserver` *`vserver_name`*
Todas as definições do GPO	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Informações relacionadas

Como os GPOs são atualizados no servidor CIFS

Apresentar informações sobre as configurações do GPO

Você pode exibir informações sobre configurações de GPO (Group Policy Object) definidas no ative Directory e sobre configurações GPO aplicadas ao servidor CIFS.

Sobre esta tarefa

Você pode exibir informações sobre todas as configurações de GPO definidas no ative Directory do domínio ao qual o servidor CIFS pertence, ou você pode exibir informações apenas sobre as configurações de GPO aplicadas a um servidor CIFS.

Passos

1. Exiba informações sobre as configurações do GPO executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as configurações de Diretiva de Grupo…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Aplicado a uma máquina virtual de storage habilitada por CIFS (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe as configurações de GPO definidas no ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
```

```
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
```

```
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

O exemplo a seguir exibe as configurações de GPO aplicadas ao SVM VS1 habilitado para CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
```

```
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
```

```
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Exibir informações detalhadas sobre GPOs de grupo restrito

Você pode exibir informações detalhadas sobre grupos restritos definidos como objetos de Diretiva de Grupo (GPOs) no ative Directory e aplicados ao servidor CIFS.

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome da política de grupo
- Versão da política de grupo
- Link

  Especifica o nível no qual a diretiva de grupo está configurada. Os possíveis valores de saída incluem o seguinte:

  - `Local` Quando a política de grupo é configurada no ONTAP
  - `Site` quando a política de grupo é configurada no nível do site no controlador de domínio
  - `Domain` quando a política de grupo é configurada no nível do domínio no controlador de domínio
  - `OrganizationalUnit` Quando a política de grupo é configurada no nível de unidade organizacional (ou) no controlador de domínio
  - `RSOP` para o conjunto resultante de políticas derivadas de todas as políticas de grupo definidas em vários níveis
- Nome do grupo restrito
- Os usuários e grupos que pertencem e que não pertencem ao grupo restrito

- A lista de grupos aos quais o grupo restrito é adicionado

  Um grupo pode ser membro de grupos que não sejam os listados aqui.

Passo

1. Exiba informações sobre todos os GPOs de grupo restrito executando uma das seguintes ações:

Se você quiser exibir informações sobre todos os GPOs de grupo restrito…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações sobre GPOs de grupo restrito definidos no domínio do ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

O exemplo a seguir exibe informações sobre GPOs de grupos restritos aplicados ao SVM VS1 habilitado para CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibir informações sobre políticas de acesso centrais

Você pode exibir informações detalhadas sobre as políticas de acesso central definidas no ative Directory. Você também pode exibir informações sobre as políticas de acesso central aplicadas ao servidor CIFS por meio de objetos de diretiva de grupo (GPOs).

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da política de acesso central
- SID
- Descrição
- Tempo de criação
- Tempo de modificação
- Regras dos membros

> Os servidores CIFS no modo de grupo de trabalho não são exibidos porque não suportam GPOs.

Passo

1. Exiba informações sobre políticas de acesso central executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

Exemplo

O exemplo a seguir exibe informações de todas as políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
------------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

O exemplo a seguir exibe informações de todas as políticas de acesso central aplicadas às máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre as regras da política de acesso central

Exibir informações sobre as regras da política de acesso central

Você pode exibir informações detalhadas sobre regras de política de acesso central associadas a políticas de acesso centrais definidas no ative Directory. Você também pode exibir informações sobre regras de políticas de acesso centrais aplicadas ao servidor CIFS por meio de GPOs de diretiva de acesso central (objetos de diretiva de grupo).

Sobre esta tarefa

Você pode exibir informações detalhadas sobre regras de política de acesso central definidas e aplicadas. Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da regra de acesso central
- Descrição
- Tempo de criação
- Tempo de modificação
- Permissões atuais

- Permissões propostas
- Direcionar recursos

Se você quiser exibir informações sobre todas as regras de política de acesso central associadas às políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central aplicadas a máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Comandos para gerenciar senhas de contas de computador de servidores SMB

Você precisa saber os comandos para alterar, redefinir e desativar senhas e para configurar agendas de atualização automática. Você também pode configurar um agendamento no servidor SMB para atualizá-lo automaticamente.

Se você quiser…	Use este comando…
Altere a senha da conta de domínio quando o ONTAP estiver sincronizado com os serviços do AD	`vserver cifs domain password change`
Redefina a senha da conta de domínio quando o ONTAP não estiver sincronizado com os serviços do AD	`vserver cifs domain password reset`
Configurar servidores SMB para alterações automáticas de senha de conta de computador	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`

Se você quiser…	Use este comando…
Desativar alterações automáticas de senha de conta de computador em servidores SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Consulte a página de manual de cada comando para obter mais informações.

Gerenciar conexões do controlador de domínio

Exibir informações sobre servidores descobertos

Você pode exibir informações relacionadas a servidores LDAP e controladores de domínio descobertos em seu servidor CIFS.

Passo

1. Para exibir informações relacionadas aos servidores descobertos, digite o seguinte comando: `vserver cifs domain discovered-servers show`

Exemplo

O exemplo a seguir mostra os servidores descobertos para o SVM VS1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informações relacionadas

Redefinir e redescobrir servidores

Parar ou iniciar o servidor CIFS

Redefinir e redescobrir servidores

Redefinir e redescobrir servidores no servidor CIFS permite que o servidor CIFS descarte informações armazenadas sobre servidores LDAP e controladores de domínio. Depois de descartar as informações do servidor, o servidor CIFS readquire as informações atuais sobre esses servidores externos. Isso pode ser útil quando os servidores conetados não estão respondendo adequadamente.

Passos

1. Introduza o seguinte comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Exibir informações sobre os servidores recém-redescobertos: `vserver cifs domain discovered-servers show -vserver vserver_name`

Exemplo

O exemplo a seguir redefine e redescobre servidores para máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informações relacionadas

Exibindo informações sobre servidores descobertos

Parar ou iniciar o servidor CIFS

Gerenciar a descoberta do controlador de domínio

A partir do ONTAP 9.3, você pode modificar o processo padrão pelo qual controladores de domínio (DCs) são descobertos. Isso permite limitar a descoberta ao seu site ou a um pool de DCs preferenciais, o que pode levar a melhorias de desempenho, dependendo do ambiente.

Sobre esta tarefa

Por padrão, o processo de descoberta dinâmica descobre todos os DCs disponíveis, incluindo todos os DCs preferenciais, todos os DCs no local e todos os DCs remotos. Essa configuração pode levar à latência na autenticação e ao acesso a compartilhamentos em determinados ambientes. Se você já determinou o pool de DCs que deseja usar, ou se os DCs remotos são inadequados ou inacessíveis, você pode alterar o método de descoberta.

No ONTAP 9.3 e versões posteriores, o `discovery-mode` parâmetro `cifs domain discovered-servers` do comando permite selecionar uma das seguintes opções de descoberta:

- Todos os DCs no domínio são descobertos.

- Apenas DCs no local são descobertos.

  O `default-site` parâmetro para o servidor SMB pode ser definido para usar esse modo com LIFs que não são atribuídos a um site em sites e serviços.

- A deteção de servidor não é realizada, a configuração do servidor SMB depende apenas de DCs preferenciais.

  Para utilizar este modo, tem de definir primeiro os DCs preferidos para o servidor SMB.

Antes de começar

Você deve estar no nível de privilégio avançado.

Passo

1. Especifique a opção de descoberta desejada: `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   Opções para o `mode` parâmetro:

   - `all`

     Descubra todos os DCs disponíveis (padrão).

   - `site`

     Limite a descoberta DC ao seu site.

   - `none`

     Use apenas DCs preferenciais e não execute a descoberta.

Adicione controladores de domínio preferenciais

O ONTAP descobre automaticamente controladores de domínio através do DNS. Opcionalmente, você pode adicionar um ou mais controladores de domínio à lista de controladores de domínio preferenciais para um domínio específico.

Sobre esta tarefa

Se já existir uma lista de controlador de domínio preferencial para o domínio especificado, a nova lista será mesclada com a lista existente.

Passo

1. Para adicionar à lista de controladores de domínio preferenciais, digite o seguinte comando `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* Especifica o nome da máquina virtual de storage (SVM).

   `-domain` *`domain_name`* Especifica o nome totalmente qualificado do ative Directory do domínio ao qual pertencem os controladores de domínio especificados.

`-preferred-dc IP_address`,... especifica um ou mais endereços IP dos controladores de domínio preferidos, como uma lista delimitada por vírgulas, por ordem de preferência.

Exemplo

O comando a seguir adiciona controladores de domínio 172.17.102.25 e 172.17.102.24 à lista de controladores de domínio preferenciais que o servidor SMB no SVM VS1 usa para gerenciar o acesso externo ao domínio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informações relacionadas

Comandos para gerenciar controladores de domínio preferenciais

Comandos para gerenciar controladores de domínio preferenciais

Você precisa saber os comandos para adicionar, exibir e remover controladores de domínio preferenciais.

Se você quiser…	Use este comando…
Adicione um controlador de domínio preferido	`vserver cifs domain preferred-dc add`
Exibir controladores de domínio preferenciais	`vserver cifs domain preferred-dc show`
Remova um controlador de domínio preferido	`vserver cifs domain preferred-dc remove`

Consulte a página de manual de cada comando para obter mais informações.

Informações relacionadas

Adicionando controladores de domínio preferenciais

Ative as conexões SMB2 aos controladores de domínio

A partir do ONTAP 9.1, você pode habilitar o SMB versão 2,0 para se conetar a um controlador de domínio. Isso é necessário se você desativou o SMB 1,0 em controladores de domínio. A partir do ONTAP 9.2, o SMB2 é ativado por predefinição.

Sobre esta tarefa

A `smb2-enabled-for-dc-connections` opção de comando ativa o padrão do sistema para o lançamento do ONTAP que você está usando. O padrão do sistema para o ONTAP 9.1 está ativado para o SMB 1,0 e desativado para o SMB 2,0. O padrão do sistema para o ONTAP 9.2 está habilitado para o SMB 1,0 e habilitado para o SMB 2,0. Se o controlador de domínio não puder negociar o SMB 2,0 inicialmente, ele usará o SMB 1,0.

O SMB 1,0 pode ser desativado do ONTAP para um controlador de domínio. No ONTAP 9.1, se o SMB 1,0 tiver sido desativado, o SMB 2,0 deve ser ativado para se comunicar com um controlador de domínio.

Saiba mais sobre:

- "Verificando versões SMB ativadas".
- "Versões e funcionalidade SMB compatíveis".

> Se `-smb1-enabled-for-dc-connections` estiver definido como `false` enquanto `-smb1-enabled` estiver definido como `true`, o ONTAP nega conexões SMB 1,0 como cliente, mas continua a aceitar conexões SMB 1,0 de entrada como servidor.

Passos

1. Antes de alterar as configurações de segurança SMB, verifique quais versões SMB estão ativadas: `vserver cifs security show`
2. Role a lista para baixo para ver as versões SMB.
3. Execute o comando apropriado, usando a `smb2-enabled-for-dc-connections` opção.

Se você quiser que SMB2 seja…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc-connections true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc-connections false`

Ative conexões criptografadas para controladores de domínio

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas.

Sobre esta tarefa

O ONTAP requer criptografia para comunicações de controlador de domínio (DC) quando a `-encryption-required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3.

Quando as comunicações CC criptografadas são necessárias, a `-smb2-enabled-for-dc-connections` opção é ignorada, porque o ONTAP negocia somente conexões SMB3. Se um DC não suportar SMB3 e criptografia, o ONTAP não se conetará a ele.

Passo

1. Ative a comunicação encriptada com o DC: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Use sessões nulas para acessar o armazenamento em ambientes não Kerberos

Use sessões nulas para acessar o armazenamento na visão geral de ambientes não Kerberos

O acesso de sessão nula fornece permissões para recursos de rede, como dados do sistema de armazenamento de dados, e para serviços baseados em cliente executados no sistema local. Uma sessão nula ocorre quando um processo de cliente usa a conta "system" para acessar um recurso de rede. A configuração de sessão nula é específica para autenticação não Kerberos.

Como o sistema de armazenamento fornece acesso nulo à sessão

Como compartilhamentos de sessão nulos não exigem autenticação, os clientes que exigem acesso de sessão null devem ter seus endereços IP mapeados no sistema de armazenamento.

Por padrão, os clientes de sessão nula não mapeados podem acessar determinados serviços do sistema ONTAP, como enumeração de compartilhamento, mas eles são restritos a acessar quaisquer dados do sistema de storage.

> O ONTAP suporta os valores de configuração do Registro anônimo do Windows com a `-restrict-anonymous` opção. Isso permite controlar até que ponto os usuários nulos não mapeados podem exibir ou acessar recursos do sistema. Por exemplo, você pode desativar a enumeração de compartilhamento e o acesso ao compartilhamento IPC (o compartilhamento de pipe nomeado oculto). As `vserver cifs options modify` páginas de manual e `vserver cifs options show` fornecem mais informações sobre a `-restrict-anonymous` opção.

A menos que configurado de outra forma, um cliente executando um processo local que solicita acesso ao sistema de armazenamento por meio de uma sessão nula é membro apenas de grupos não restritivos, como "'todos'". Para limitar o acesso de sessão nula a recursos selecionados do sistema de armazenamento, você pode querer criar um grupo ao qual todos os clientes de sessão nula pertencem; a criação deste grupo permite restringir o acesso ao sistema de armazenamento e definir permissões de recursos do sistema de armazenamento que se aplicam especificamente a clientes de sessão nula.

O ONTAP fornece uma sintaxe de mapeamento no `vserver name-mapping` conjunto de comandos para especificar o endereço IP dos clientes que têm acesso permitido aos recursos do sistema de armazenamento usando uma sessão de usuário nula. Depois de criar um grupo para usuários nulos, você pode especificar restrições de acesso para recursos do sistema de armazenamento e permissões de recursos que se aplicam somente a sessões nulas. O usuário nulo é identificado como logon anônimo. Os usuários nulos não têm acesso a nenhum diretório home.

Qualquer usuário nulo que acesse o sistema de armazenamento a partir de um endereço IP mapeado recebe permissões de usuário mapeadas. Considere as precauções apropriadas para evitar o acesso não autorizado aos sistemas de armazenamento mapeados com usuários nulos. Para máxima proteção, coloque o sistema de armazenamento e todos os clientes que necessitem de acesso nulo ao sistema de armazenamento de utilizadores numa rede separada, para eliminar a possibilidade de "spoofing" de endereço IP.

Informações relacionadas

Configurando restrições de acesso para usuários anônimos

Conceder acesso a usuários nulos a compartilhamentos de sistema de arquivos

Você pode permitir o acesso aos recursos do seu sistema de armazenamento por clientes de sessão nulos, atribuindo um grupo a ser usado por clientes de sessão nulos e

registrando os endereços IP de clientes de sessão nulos para adicionar à lista de clientes com permissão para acessar dados usando sessões nulas.

Passos

1. Use o `vserver name-mapping create` comando para mapear o usuário nulo para qualquer usuário válido do Windows, com um qualificador IP.

   O comando a seguir mapeia o usuário nulo para user1 com um nome de host válido google.com:

   ```
   vserver name-mapping create –direction win-unix  -position 1 –pattern
   “ANONYMOUS LOGON” –replacement user1 – hostname google.com
   ```

   O comando a seguir mapeia o usuário nulo para user1 com um endereço IP válido 10.238.2.54/32:

   ```
   vserver name-mapping create –direction win-unix  -position 2 –pattern
   “ANONYMOUS LOGON” –replacement user1 –address 10.238.2.54/32
   ```

2. Use o `vserver name-mapping show` comando para confirmar o mapeamento de nomes.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Use o `vserver cifs options modify –win-name-for-null-user` comando para atribuir a associação do Windows ao usuário nulo.

   Essa opção é aplicável somente quando há um mapeamento de nome válido para o usuário nulo.

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. Use o `vserver cifs options show` comando para confirmar o mapeamento do usuário nulo para o usuário ou grupo do Windows.

   ```
   vserver cifs options show

   Vserver :vs1

   Map Null User to Windows User of Group: user1
   ```

Gerencie aliases NetBIOS para servidores SMB

Gerenciar aliases NetBIOS para servidores SMB

Os aliases NetBIOS são nomes alternativos para o servidor SMB que os clientes SMB podem usar ao se conetar ao servidor SMB. A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores de arquivos originais.

Você pode especificar uma lista de aliases NetBIOS ao criar o servidor SMB ou a qualquer momento depois de criar o servidor SMB. Você pode adicionar ou remover aliases NetBIOS da lista a qualquer momento. Você pode se conetar ao servidor SMB usando qualquer um dos nomes na lista de alias do NetBIOS.

Informações relacionadas

Exibindo informações sobre NetBIOS sobre conexões TCP

Adicione uma lista de aliases NetBIOS ao servidor SMB

Se você quiser que os clientes SMB se conetem ao servidor SMB usando um alias, você pode criar uma lista de aliases NetBIOS ou adicionar aliases NetBIOS a uma lista existente de aliases NetBIOS.

Sobre esta tarefa

- O nome de alias NetBIOS pode ter 15 até carateres de comprimento.
- Você pode configurar até 200 aliases NetBIOS no servidor SMB.
- Não são permitidos os seguintes carateres:
- ( ) [ ] | ; : " , > / ?

Passos

1. Adicione os aliases NetBIOS
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Você pode especificar um ou mais aliases NetBIOS usando uma lista delimitada por vírgulas.
   - Os aliases NetBIOS especificados são adicionados à lista existente.
   - Uma nova lista de aliases NetBIOS é criada se a lista estiver vazia no momento.
2. Verifique se os aliases NetBIOS foram adicionados corretamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Informações relacionadas

Removendo aliases NetBIOS da lista de alias NetBIOS

Exibindo a lista de aliases NetBIOS em servidores CIFS

Remova os aliases NetBIOS da lista de alias NetBIOS

Se você não precisar de aliases NetBIOS específicos para um servidor CIFS, você poderá remover esses aliases NetBIOS da lista. Você também pode remover todos os aliases NetBIOS da lista.

Sobre esta tarefa

Você pode remover mais de um alias NetBIOS usando uma lista delimitada por vírgulas. Você pode remover todos os aliases NetBIOS em um servidor CIFS especificando - como o valor para o `-netbios-aliases` parâmetro.

Passos

1. Execute uma das seguintes ações:

Se você quiser remover…	Digite…
Aliases NetBIOS específicos da lista	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Todos os aliases NetBIOS da lista	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verifique se os aliases NetBIOS especificados foram removidos: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Exiba a lista de aliases NetBIOS em servidores CIFS

Você pode exibir a lista de aliases NetBIOS. Isso pode ser útil quando você deseja determinar a lista de nomes sobre os quais clientes SMB podem fazer conexões com o servidor CIFS.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite…
Os aliases NetBIOS de um servidor CIFS	`vserver cifs show -display-netbios -aliases`
A lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS	`vserver cifs show -instance`

O exemplo a seguir exibe informações sobre os aliases NetBIOS de um servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

O exemplo a seguir exibe a lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS:

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
               CIFS Server Administrative Status: up
                         CIFS Server Description:
                         List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Consulte a página de manual para obter mais informações.

Informações relacionadas

Adicionando uma lista de aliases NetBIOS ao servidor CIFS

Determine se os clientes SMB estão conetados usando aliases NetBIOS

Você pode determinar se os clientes SMB estão conetados usando aliases NetBIOS e, em caso afirmativo, qual alias NetBIOS é usado para fazer a conexão. Isso pode ser útil ao solucionar problemas de conexão.

Sobre esta tarefa

Você deve usar o `-instance` parâmetro para exibir o alias NetBIOS (se houver) associado a uma conexão SMB. Se o nome do servidor CIFS ou um endereço IP for usado para fazer a conexão SMB, a saída para o `NetBIOS Name` campo é – (hífen).

Passo

1. Execute a ação desejada:

Se você quiser exibir informações do NetBIOS para…	Digite…
Conexões SMB	`vserver cifs session show -instance`
Conexões usando um alias NetBIOS especificado:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

O exemplo a seguir exibe informações sobre o alias NetBIOS usado para fazer a conexão SMB com o Session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Gerenciar diversas tarefas de servidor SMB

Pare ou inicie o servidor CIFS

Você pode parar o servidor CIFS em uma SVM, que pode ser útil na execução de tarefas enquanto os usuários não acessam dados por compartilhamentos SMB. Você pode reiniciar o acesso SMB iniciando o servidor CIFS. Ao parar o servidor CIFS, você também pode modificar os protocolos permitidos na máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Pare o servidor CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Inicie o servidor CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` especifica se o comando deve ser executado em primeiro plano ou em segundo plano. Se você não inserir esse parâmetro, ele será definido como `true`, e o comando será executado em primeiro plano.

2. Verifique se o status administrativo do servidor CIFS está correto usando o `vserver cifs show` comando.

Exemplo

Os comandos a seguir iniciam o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Informações relacionadas

Exibindo informações sobre servidores descobertos

Redefinir e redescobrir servidores

Mova servidores CIFS para diferentes OUs

O processo de criação do servidor CIFS usa a unidade organizacional padrão (ou) CN de computadores durante a configuração, a menos que você especifique uma ou diferente. Você pode mover servidores CIFS para diferentes OUs após a configuração.

Passos

1. No servidor Windows, abra a árvore **usuários e computadores do ative Directory**.
2. Localize o objeto do ative Directory da máquina virtual de storage (SVM).
3. Clique com o botão direito do rato no objeto e selecione **mover**.
4. Selecione a UO que você deseja associar ao SVM

Resultados

O objeto SVM é colocado na UO selecionada.

Modifique o domínio DNS dinâmico na SVM antes de mover o servidor SMB

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS do servidor SMB no DNS ao mover o servidor SMB para outro domínio, você deve modificar DNS dinâmico (DDNS) na máquina virtual de armazenamento (SVM) antes de mover o servidor SMB.

Antes de começar

Os serviços de nomes DNS devem ser modificados no SVM para usar o domínio DNS que contém os

Registros de localização do serviço para o novo domínio que conterá a conta de computador do servidor SMB. Se você estiver usando DDNS seguro, você deve usar servidores de nomes DNS integrados ao ative Directory.

Sobre esta tarefa

Embora o DDNS (se configurado no SVM) adicione automaticamente os Registros DNS para LIFs de dados ao novo domínio, os Registros DNS para o domínio original não são excluídos automaticamente do servidor DNS original. Você deve excluí-los manualmente.

Para concluir as modificações do DDNS antes de mover o servidor SMB, consulte o seguinte tópico:

"Configurar serviços DNS dinâmicos"

Ingressar em um SVM em um domínio do active Directory

É possível associar uma máquina virtual de armazenamento (SVM) a um domínio do ative Directory sem excluir o servidor SMB existente, modificando o domínio usando o `vserver cifs modify` comando. Você pode ingressar novamente no domínio atual ou ingressar em um novo.

Antes de começar

- O SVM já deve ter uma configuração de DNS.
- A configuração DNS do SVM deve ser capaz de servir o domínio de destino.

  Os servidores DNS têm de conter os registos de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio.

Sobre esta tarefa

- O status administrativo do servidor CIFS deve ser definido como "próprio" para prosseguir com a modificação de domínio do ative Directory.
- Se o comando for concluído com êxito, o status administrativo será automaticamente definido como "'up"'.
- Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

Passos

1. Junte-se ao SVM ao domínio do servidor CIFS: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Para obter mais informações, consulte a página man para o `vserver cifs modify` comando. Se você precisar reconfigurar o DNS para o novo domínio, consulte a página de manual do `vserver dns modify` comando.

   Para criar uma conta de máquina do ative Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=` *`example`* `ou` contentor dentro do *`example`* domínio .com.

   A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

2. Verifique se o servidor CIFS está no domínio desejado do ative Directory: `vserver cifs show`

Exemplo

No exemplo a seguir, o servidor SMB "'CIFSSERVER1"" no SVM VS1 junta o domínio example.com usando autenticação keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

Exibir informações sobre NetBIOS sobre conexões TCP

Você pode exibir informações sobre conexões NetBIOS sobre TCP (NBT). Isso pode ser útil ao solucionar problemas relacionados ao NetBIOS.

Passo

1. Use o `vserver cifs nbtstat` comando para exibir informações sobre NetBIOS sobre conexões TCP.

   O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Exemplo

O exemplo a seguir mostra as informações do serviço de nomes NetBIOS exibidas para "'cluster1":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Comandos para gerenciar servidores SMB

Você precisa saber os comandos para criar, exibir, modificar, parar, iniciar e excluir servidores SMB. Há também comandos para redefinir e redescobrir servidores, alterar ou redefinir senhas de conta de máquina, agendar alterações para senhas de conta de máquina e adicionar ou remover aliases NetBIOS.

Se você quiser…	Use este comando…
Crie um servidor SMB	`vserver cifs create`
Exibir informações sobre um servidor SMB	`vserver cifs show`
Modifique um servidor SMB	`vserver cifs modify`
Mova um servidor SMB para outro domínio	`vserver cifs modify`

Parar um servidor SMB	`vserver cifs stop`
Inicie um servidor SMB	`vserver cifs start`
Excluir um servidor SMB	`vserver cifs delete`
Redefinir e redescobrir servidores para o servidor SMB	`vserver cifs domain discovered-servers reset-servers`
Altere a senha da conta de máquina do servidor SMB	`vserver cifs domain password change`
Redefina a senha da conta da máquina do servidor SMB	`vserver cifs domain password change`
Agendar alterações automáticas de senha para a conta de máquina do servidor SMB	`vserver cifs domain password schedule modify`
Adicione aliases NetBIOS para o servidor SMB	`vserver cifs add-netbios-aliases`
Remova os aliases NetBIOS para o servidor SMB	`vserver cifs remove-netbios-aliases`

Consulte a página de manual de cada comando para obter mais informações.

Informações relacionadas

"O que acontece com usuários e grupos locais ao excluir servidores SMB"

Ative o serviço de nomes NetBIOS

Começando com ONTAP 9, o serviço de nomes NetBIOS (NBNS, às vezes chamado de Serviço de nomes de Internet do Windows ou WINS) é desativado por padrão. Anteriormente, as máquinas virtuais de armazenamento (SVMs) habilitadas por CIFS enviavam transmissões de Registro de nomes, independentemente de o WINS estar habilitado em uma rede. Para limitar tais transmissões a configurações em que o NBNS é necessário, você deve habilitar o NBNS explicitamente para novos servidores CIFS.

Antes de começar

- Se você já estiver usando NBNS e atualizar para o ONTAP 9, não é necessário concluir esta tarefa. NBNS continuará a funcionar como antes.
- O NBNS é ativado por UDP (porta 137).
- NBNS sobre IPv6 não é suportado.

Passos

1. Defina o nível de privilégio como avançado.

```
set -privilege advanced
```

2. Ative NBNS em um servidor CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Retorne ao nível de privilégio de administrador.

```
set -privilege admin
```

Use o IPv6 para acesso SMB e serviços SMB

Requisitos para usar IPv6

Antes de poder usar o IPv6 no servidor SMB, você precisa saber quais versões do ONTAP e SMB o suportam e quais são os requisitos de licença.

Requisitos de licença do ONTAP

Nenhuma licença especial é necessária para o IPv6 quando o SMB é licenciado. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

Requisitos de versão do protocolo SMB

- Para SVMs, o ONTAP oferece suporte a IPv6 em todas as versões do protocolo SMB.

O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Suporte para IPv6 com acesso SMB e serviços CIFS

Se você quiser usar o IPv6 em seu servidor CIFS, você precisa estar ciente de como o ONTAP suporta o IPv6 para acesso SMB e comunicação de rede para serviços CIFS.

Suporte ao cliente e servidor Windows

O ONTAP fornece suporte para servidores e clientes Windows que suportam IPv6. A seguir descreve o suporte ao cliente e servidor Microsoft Windows IPv6:

- O Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 e posterior suportam o IPv6 para serviços de partilha de ficheiros SMB e ative Directory, incluindo DNS, LDAP, CLDAP e Kerberos.

  Se os endereços IPv6 estiverem configurados, o Windows 7 e o Windows Server 2008 e versões posteriores usam o IPv6 por padrão para serviços do ative Directory. Tanto a autenticação NTLM como Kerberos através de conexões IPv6 são suportadas.

Todos os clientes Windows suportados pelo ONTAP podem se conetar a compartilhamentos SMB usando endereços IPv6.

Para obter as informações mais recentes sobre quais clientes Windows ONTAP suportam, consulte "Matriz de interoperabilidade".

Os domínios NT não são suportados para IPv6.

Suporte adicional a serviços CIFS

Além do suporte IPv6 para compartilhamentos de arquivos SMB e serviços do ative Directory, o ONTAP oferece suporte IPv6 para o seguinte:

- Serviços do lado do cliente, incluindo pastas offline, perfis de roaming, redirecionamento de pastas e versões anteriores
- Serviços do lado do servidor, incluindo diretórios base dinâmicos (recurso Home Directory), links simbólicos e Widelinks, BranchCache, descarga de cópia ODX, referências automáticas de nós e versões anteriores
- Serviços de gerenciamento de acesso a arquivos, incluindo o uso de usuários e grupos locais do Windows para controle de acesso e gerenciamento de direitos, configuração de permissões de arquivos e políticas de auditoria usando a CLI, rastreamento de segurança, gerenciamento de bloqueios de arquivos e monitoramento de atividades SMB
- Auditoria multiprotocolo nas
- FPolicy
- Compartilhamentos continuamente disponíveis, protocolo de testemunha e VSS remoto (usado com configurações Hyper-V em SMB)

Serviço de nomes e suporte de serviços de autenticação

A comunicação com os seguintes serviços de nome é suportada com o IPv6:

- Controladores de domínio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

Como os servidores CIFS usam o IPv6 para se conetar a servidores externos

Para criar uma configuração que atenda aos seus requisitos, você deve estar ciente de como os servidores CIFS usam o IPv6 ao fazer conexões com servidores externos.

- Seleção do endereço de origem

  Se for feita uma tentativa de ligação a um servidor externo, o endereço de origem selecionado tem de ser do mesmo tipo que o endereço de destino. Por exemplo, se estiver conetando a um endereço IPv6, a máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS deve ter um LIF de dados ou LIF de gerenciamento que tenha um endereço IPv6 para usar como endereço de origem. Da mesma forma, se estiver conetando a um endereço IPv4, o SVM precisa ter um LIF de dados ou um LIF de gerenciamento

que tenha um endereço IPv4 para usar como endereço de origem.

- Para servidores dinamicamente descobertos usando DNS, a descoberta do servidor é executada da seguinte forma:
  - Se o IPv6 estiver desativado no cluster, apenas serão detetados IPv4 endereços de servidores.
  - Se IPv6 estiver ativado no cluster, os endereços de servidor IPv4 e IPv6 serão descobertos. Qualquer tipo pode ser usado dependendo da adequação do servidor ao qual o endereço pertence e da disponibilidade de dados IPv6 ou IPv4 ou LIFs de gerenciamento. A descoberta dinâmica de servidor é usada para descobrir controladores de domínio e seus serviços associados, como LSA, NETLOGON, Kerberos e LDAP.
- Conetividade do servidor DNS

  Se o SVM usa IPv6 ao se conetar a um servidor DNS depende da configuração dos serviços de nome DNS. Se os serviços DNS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes DNS pode usar endereços IPv4 para que as conexões com servidores DNS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes DNS.

- Conetividade do servidor LDAP

  Se o SVM usa IPv6 ao se conetar a um servidor LDAP depende da configuração do cliente LDAP. Se o cliente LDAP estiver configurado para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração do cliente LDAP pode usar endereços IPv4 para que as conexões com servidores LDAP continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar a configuração do cliente LDAP.

  > A configuração do cliente LDAP é usada ao configurar o LDAP para serviços de nome de usuário, grupo e netgroup UNIX.

- Conetividade do servidor NIS

  Se o SVM usa IPv6 ao conetar-se a um servidor NIS depende da configuração dos serviços de nome NIS. Se os serviços NIS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes NIS pode usar endereços IPv4 para que as conexões com servidores NIS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes NIS.

  > Os serviços de nomes NIS são usados para armazenar e gerenciar objetos de nome de usuário, grupo, netgroup e host UNIX.

Informações relacionadas

Habilitação do IPv6 para SMB (somente administradores de cluster)

Monitoramento e exibição de informações sobre IPv6 sessões SMB

Ativar o IPv6 para SMB (somente administradores de cluster)

As redes IPv6 não estão ativadas durante a configuração do cluster. Um administrador de cluster deve habilitar o IPv6 após a conclusão da configuração do cluster para usar o IPv6 para SMB. Quando o administrador do cluster ativa o IPv6, ele é ativado para todo o cluster.

Passo

1. Ativar IPv6: `network options ipv6 modify -enabled true`

   Para obter mais informações sobre como ativar o IPv6 no cluster e configurar LIFs IPv6, consulte o *Network Management Guide*.

   IPv6 está ativado. LIFs de dados IPv6 para acesso SMB podem ser configurados.

Informações relacionadas

Monitoramento e exibição de informações sobre IPv6 sessões SMB

"Gerenciamento de rede"

Desativar IPv6 para SMB

Mesmo que IPv6 esteja habilitado no cluster usando uma opção de rede, você não pode desabilitar IPv6 para SMB usando o mesmo comando. Em vez disso, o ONTAP desativa o IPv6 quando o administrador do cluster desativa a última interface habilitada para IPv6 no cluster. Você deve se comunicar com o administrador do cluster sobre o gerenciamento de suas interfaces IPv6 habilitadas.

Para obter mais informações sobre a desativação do IPv6 no cluster, consulte o *Network Management Guide*.

Informações relacionadas

"Gerenciamento de rede"

Monitore e exiba informações sobre IPv6 sessões SMB

Você pode monitorar e exibir informações sobre sessões SMB conetadas usando redes IPv6G. Essas informações são úteis para determinar quais clientes estão se conetando usando o IPv6, bem como outras informações úteis sobre sessões SMB do IPv6.

Passo

1. Execute a ação desejada:

Se você quiser determinar se…	Digite o comando…
As sessões de SMB a uma máquina virtual de storage (SVM) são conetadas usando o IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 é usado para sessões SMB através de um endereço LIF especificado	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* É o endereço IPv6 do LIF de dados.

Configure o acesso a arquivos usando SMB

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Estilos de segurança e seus efeitos

Existem quatro estilos de segurança diferentes: UNIX, NTFS, misto e unificado. Cada estilo de segurança tem um efeito diferente sobre como as permissões são tratadas para os dados. Você deve entender os diferentes efeitos para garantir que você selecione o estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar dados. Os estilos de segurança determinam apenas o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e que tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa estilo de segurança UNIX, os clientes SMB ainda podem acessar dados (desde que autentiquem e autorizem adequadamente) devido à natureza multiprotocolo do ONTAP. No entanto, o ONTAP usa permissões UNIX que somente clientes UNIX podem modificar usando ferramentas nativas.

Estilo de segurança	Clientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Clientes que podem acessar arquivos
UNIX	NFS	NFSv3 bits de modo	UNIX	NFS e SMB
		ACLs NFSv4.x		
NTFS	SMB	ACLs NTFS	NTFS	
Misto	NFS ou SMB	NFSv3 bits de modo	UNIX	
		NFSv4.ACLs		
		ACLs NTFS	NTFS	
Unificado (somente para volumes infinitos, no ONTAP 9.4 e versões anteriores).	NFS ou SMB	NFSv3 bits de modo	UNIX	
		ACLs NFSv4,1		
		ACLs NTFS	NTFS	

Os volumes FlexVol suportam estilos de segurança UNIX, NTFS e mistos. Quando o estilo de segurança é misto ou unificado, as permissões efetivas dependem do tipo de cliente que modificou as permissões pela última vez porque os usuários definem o estilo de segurança individualmente. Se o último cliente que modificou permissões fosse um cliente NFSv3, as permissões são bits do modo UNIX NFSv3. Se o último cliente foi um cliente NFSv4, as permissões são NFSv4 ACLs. Se o último cliente foi um cliente SMB, as permissões são ACLs do Windows NTFS.

O estilo de segurança unificado só está disponível com volumes infinitos, que não são mais suportados no ONTAP 9.5 e versões posteriores. Para obter mais informações, Visão geral do gerenciamento do FlexGroup volumesconsulte .

A partir do ONTAP 9.2, o `show-effective-permissions` parâmetro para o `vserver security file-`

`directory` comando permite exibir permissões efetivas concedidas a um usuário Windows ou UNIX no caminho especificado de arquivo ou pasta. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo.

> O ONTAP define inicialmente algumas permissões de arquivo padrão. Por padrão, o estilo de segurança eficaz em todos os dados em UNIX, volumes mistos e de estilo de segurança unificado é UNIX e o tipo de permissões efetivas é bits de modo UNIX (0755 a menos que especificado de outra forma) até ser configurado por um cliente como permitido pelo estilo de segurança padrão. Por padrão, o estilo de segurança eficaz em todos os dados em volumes de estilo de segurança NTFS é NTFS e tem uma ACL que permite o controle total para todos.

Onde e quando definir estilos de segurança

Os estilos de segurança podem ser definidos em volumes FlexVol (raiz ou volumes de dados) e qtrees. Os estilos de segurança podem ser definidos manualmente no momento da criação, herdados automaticamente ou alterados posteriormente.

Decida qual estilo de segurança usar em SVMs

Para ajudá-lo a decidir qual estilo de segurança usar em um volume, você deve considerar dois fatores. O fator principal é o tipo de administrador que gerencia o sistema de arquivos. O fator secundário é o tipo de usuário ou serviço que acessa os dados no volume.

Ao configurar o estilo de segurança em um volume, você deve considerar as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança e evite problemas com o gerenciamento de permissões. As seguintes considerações podem ajudá-lo a decidir:

Estilo de segurança	Escolha se…
UNIX	• O sistema de arquivos é gerenciado por um administrador UNIX. • A maioria dos usuários são clientes NFS. • Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	• O sistema de arquivos é gerenciado por um administrador do Windows. • A maioria dos usuários são clientes SMB. • Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Como a herança de estilo de segurança funciona

Se você não especificar o estilo de segurança ao criar um novo FlexVol volume ou uma qtree, ele herdará seu estilo de segurança de maneiras diferentes.

Os estilos de segurança são herdados da seguinte maneira:

- Um FlexVol volume herda o estilo de segurança do volume raiz do SVM.
- Uma qtree herda o estilo de segurança do seu que contém FlexVol volume.
- Um arquivo ou diretório herda o estilo de segurança dele contendo FlexVol volume ou qtree.

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Configurar estilos de segurança em volumes raiz do SVM

Você configura o estilo de segurança do volume raiz da máquina virtual de storage (SVM) para determinar o tipo de permissões usado para dados no volume raiz do SVM.

Passos

1. Use o `vserver create` comando com o `-rootvolume-security-style` parâmetro para definir o estilo de segurança.

   As opções possíveis para o estilo de segurança do volume raiz são `unix`, `ntfs` ou `mixed`.

2. Exiba e verifique a configuração, incluindo o estilo de segurança do volume raiz do SVM criado: `vserver show -vserver vserver_name`

Configurar estilos de segurança no FlexVol volumes

Você configura o estilo de segurança do FlexVol volume para determinar o tipo de permissões usadas para dados nos volumes do FlexVol da máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se o FlexVol volume…	Use o comando…
Ainda não existe	`volume create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança do FlexVol volume são `unix`, `ntfs` ou `mixed`.

   Se você não especificar um estilo de segurança ao criar um FlexVol volume, o volume herdará o estilo de segurança do volume raiz.

   Para obter mais informações sobre os `volume create` comandos ou `volume modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança do FlexVol volume criado, digite o seguinte comando:

   `volume show -volume volume_name -instance`

Configurar estilos de segurança no qtrees

Você configura o estilo de segurança do volume de qtree para determinar o tipo de permissões usadas para dados no qtrees.

Passos

1. Execute uma das seguintes ações:

Se a qtree…	Use o comando…
Ainda não existe	`volume qtree create` e inclua o `-security -style` parâmetro para especificar o estilo de segurança.
Já existe	`volume qtree modify` e inclua o `-security -style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança de qtree são `unix`, `ntfs`, ou `mixed`.

   Se você não especificar um estilo de segurança ao criar uma qtree, o estilo de segurança padrão será `mixed`.

   Para obter mais informações sobre os `volume qtree create` comandos ou `volume qtree modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança da qtree que você criou, digite o seguinte comando: `volume qtree show -qtree qtree_name -instance`

Crie e gerencie volumes de dados em namespaces nas

Criar e gerenciar volumes de dados na visão geral dos namespaces nas

Para gerenciar o acesso a arquivos em um ambiente nas, você precisa gerenciar volumes de dados e pontos de junção na máquina virtual de storage (SVM). Isso inclui Planejar sua arquitetura de namespace, criar volumes com ou sem pontos de junção, montar ou desmontar volumes e exibir informações sobre volumes de dados e namespaces de servidor NFS ou CIFS.

Crie volumes de dados com pontos de junção especificados

Pode especificar o ponto de junção quando cria um volume de dados. O volume resultante é montado automaticamente no ponto de junção e está imediatamente disponível para configurar para acesso nas.

Antes de começar

O agregado no qual você deseja criar o volume já deve existir.

> Os seguintes carateres não podem ser usados no caminho de junção: * *
>
> Além disso, o comprimento do caminho de junção não pode ter mais de 255 carateres.

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   O caminho de junção deve começar com a raiz (/) e pode conter diretórios e volumes juntados. O caminho de junção não precisa conter o nome do volume. Os caminhos de junção são independentes do nome do volume.

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados criado. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   O caminho de junção é insensível a maiúsculas e minúsculas; `/ENG` é o mesmo que `/eng`. Se você criar um compartilhamento CIFS, o Windows tratará o caminho de junção como se ele fosse sensível a maiúsculas e minúsculas. Por exemplo, se a junção for `/ENG`, o caminho de um compartilhamento CIFS deve começar com `/ENG`, não `/eng`.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Crie volumes de dados sem especificar pontos de junção

Você pode criar um volume de dados sem especificar um ponto de junção. O volume resultante não é montado automaticamente e não está disponível para configuração para acesso nas. É necessário montar o volume antes de configurar compartilhamentos SMB ou exportações NFS para esse volume.

Antes de começar

O agregado no qual você deseja criar o volume já deve existir.

Passos

1. Crie o volume sem um ponto de junção usando o seguinte comando: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado sem um ponto de junção: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemplo

O exemplo a seguir cria um volume chamado "vendas" localizado no SVM VS1 que não está montado em um ponto de junção:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Montar ou desmontar volumes existentes no namespace nas

Um volume deve ser montado no namespace nas antes de poder configurar o acesso do cliente nas aos dados contidos nos volumes de máquina virtual de storage (SVM). Você pode montar um volume em um ponto de junção se ele não estiver montado no

momento. Você também pode desmontar volumes.

Sobre esta tarefa

Se você desmontar e colocar um volume off-line, todos os dados dentro do ponto de junção, incluindo dados em volumes com pontos de junção contidos no namespace do volume não montado, ficarão inacessíveis para clientes nas.

> Para interromper o acesso de cliente nas a um volume, não é suficiente simplesmente desmontar o volume. Você deve colocar o volume off-line ou tomar outras medidas para garantir que os caches de manipulação de arquivos do lado do cliente sejam invalidados. Para obter mais informações, consulte o seguinte artigo da base de dados de Conhecimento: "Os clientes NFSv3 ainda têm acesso a um volume depois de serem removidos do namespace no ONTAP"

Quando você desmontar e colocar um volume off-line, os dados dentro do volume não são perdidos. Além disso, políticas de exportação de volume existentes e compartilhamentos SMB criados no volume ou em diretórios e pontos de junção dentro do volume não montado são retidos. Se você remontar o volume não montado, os clientes nas poderão acessar os dados contidos no volume usando políticas de exportação e compartilhamentos SMB existentes.

Passos

1. Execute a ação desejada:

Se você quiser…	Digite os comandos…
Monte um volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Desmontar um volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Verifique se o volume está no estado de montagem desejado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemplos

O exemplo a seguir monta um volume chamado "vendas" localizado na SVM "VS1" no ponto de junção ""/vendas":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

O exemplo a seguir desmonta e coloca offline um volume chamado "data" localizado na SVM ""VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Apresentar informações sobre a montagem do volume e o ponto de junção

Você pode exibir informações sobre volumes montados para máquinas virtuais de armazenamento (SVMs) e os pontos de junção para os quais os volumes são montados. Você também pode determinar quais volumes não estão montados em um ponto de junção. Use essas informações para entender e gerenciar seu namespace SVM.

Passos

1. Execute a ação desejada:

Se você quiser exibir…	Digite o comando…
Informações resumidas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -junction`
Informações detalhadas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -volume volume_name -instance`

Se você quiser exibir…	Digite o comando…
Informações específicas sobre volumes montados e não montados no SVM	a. Se necessário, você pode exibir campos válidos para o `-fields` parâmetro usando o seguinte comando: `volume show -fields ?` b. Exiba as informações desejadas usando o `-fields` parâmetro: Volume show -vserver vserver_name -fieldname,…

Exemplos

O exemplo a seguir exibe um resumo dos volumes montados e não montados no SVM VS1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

O exemplo a seguir exibe informações sobre campos especificados para volumes localizados no SVM VS2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar mapeamentos de nomes

Configure a visão geral dos mapeamentos de nomes

O ONTAP usa mapeamento de nomes para mapear identidades CIFS para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades CIFS. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conetando a partir de um cliente NFS ou de um cliente CIFS.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso CIFS ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

  Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo, você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um

usuário UNIX específico e para o UID do usuário.

Como o mapeamento de nomes funciona

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

  Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

  Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário CIFS padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

  Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do ative Directory com o domínio home do servidor CIFS podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor CIFS na SVM.

- *Confiança bidirecional*

  Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor CIFS tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

  As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

  Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

  Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

- *Confiança inbound*

  Com uma confiança de entrada, o outro domínio confia no domínio home do servidor CIFS. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

  Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	• administrador	O usuário UNIX "'root'" é mapeado para o usuário chamado "'administrador'". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.

Padrão	Substituição	Resultado
*	• *	Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado. O padrão* é válido apenas para mapeamento de nomes do UNIX para o Windows, e não para o contrário.

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de carateres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie um mapeamento de nomes

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula `" "` (o caractere de espaço). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

   Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure o usuário padrão

Você pode configurar um usuário padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Configure o usuário UNIX padrão	`vserver cifs options modify -default -unix-user` *user_name*
Configure o usuário padrão do Windows	`vserver nfs modify -default-win-user` *user_name*

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`

Se você quiser…	Use este comando…
Troque a posição de dois mapeamentos de nomes Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`
Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consulte a página de manual de cada comando para obter mais informações.

Configurar pesquisas de mapeamento de nomes de vários domínios

Ative ou desative pesquisas de mapeamento de nomes de vários domínios

Com pesquisas de mapeamento de nomes de vários domínios, você pode usar um cartão selvagem (**) na parte de domínio de um nome do Windows ao configurar o usuário UNIX para o mapeamento de nome de usuário do Windows. O uso de um cartão selvagem (**) na parte do domínio do nome permite que o ONTAP pesquise todos os domínios que tenham uma confiança bidirecional com o domínio que contém a conta do computador do servidor CIFS.

Sobre esta tarefa

Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Quando uma lista de domínios confiáveis preferenciais é configurada, o ONTAP usa a lista de domínios confiáveis preferenciais em vez dos domínios confiáveis bidirecionais descobertos para realizar pesquisas de mapeamento de nomes de vários domínios.

- As pesquisas de mapeamento de nomes de vários domínios são ativadas por padrão.
- Esta opção está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você deseja que as pesquisas de mapeamento de nomes de vários domínios sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor SMB disponíveis

Redefinir e redescobrir domínios confiáveis

Você pode forçar a redescoberta de todos os domínios confiáveis. Isso pode ser útil quando os servidores de domínio confiáveis não estão respondendo adequadamente ou as relações de confiança foram alteradas. Somente domínios com confiança bidirecional com o domínio home, que é o domínio que contém a conta de computador do servidor CIFS, são descobertos.

Passo

1. Redefina e redescubra domínios confiáveis usando o `vserver cifs domain trusts rediscover` comando.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Informações relacionadas

Exibindo informações sobre domínios confiáveis descobertos

Exibir informações sobre domínios confiáveis descobertos

Você pode exibir informações sobre os domínios confiáveis descobertos para o domínio doméstico do servidor CIFS, que é o domínio que contém a conta de computador do servidor CIFS. Isso pode ser útil quando você quiser saber quais domínios confiáveis são descobertos e como eles são solicitados na lista de domínios confiáveis descobertos.

Sobre esta tarefa

Apenas os domínios com confiança bidirecional com o domínio home são descobertos. Como o controlador de domínio (DC) do domínio home retorna a lista de domínios confiáveis em uma ordem determinada pelo DC, a ordem dos domínios dentro da lista não pode ser prevista. Ao exibir a lista de domínios confiáveis, você pode determinar a ordem de pesquisa para pesquisas de mapeamento de nomes de vários domínios.

As informações de domínio confiável exibidas são agrupadas por nó e máquina virtual de armazenamento (SVM).

Passo

1. Exiba informações sobre domínios confiáveis descobertos usando o `vserver cifs domain trusts show` comando.

   `vserver cifs domain trusts show -vserver vs1`

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Informações relacionadas

Redefinir e redescobrir domínios confiáveis

Adicione, remova ou substitua domínios confiáveis em listas de domínios confiáveis preferenciais

Pode adicionar ou remover domínios fidedignos da lista de domínios fidedignos preferidos para o servidor SMB ou pode modificar a lista atual. Se você configurar uma lista de domínio confiável preferencial, essa lista será usada em vez dos domínios confiáveis bidirecionais descobertos ao executar pesquisas de mapeamento de nomes de vários domínios.

Sobre esta tarefa

- Se você estiver adicionando domínios confiáveis a uma lista existente, a nova lista será mesclada com a lista existente com as novas entradas colocadas no final Os domínios confiáveis são pesquisados na ordem em que aparecem na lista de domínios confiáveis.
- Se você estiver removendo domínios confiáveis da lista existente e não especificar uma lista, toda a lista de domínio confiável para a máquina virtual de armazenamento especificada (SVM) será removida.
- Se você modificar a lista existente de domínios confiáveis, a nova lista substituirá a lista existente.

Você deve inserir apenas domínios bidirecionalmente confiáveis na lista de domínios confiáveis preferidos. Mesmo que você possa inserir domínios confiáveis de saída ou entrada na lista de domínios preferidos, eles não são usados ao realizar pesquisas de mapeamento de nomes de vários domínios. O ONTAP pula a entrada do domínio unidirecional e passa para o próximo domínio confiável bidirecional na lista.

Passo

1. Execute uma das seguintes ações:

Se você quiser fazer o seguinte com a lista de domínios confiáveis preferenciais…	Use o comando…
Adicione domínios confiáveis à lista	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Remova domínios confiáveis da lista	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifique a lista existente	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Exemplos

O comando a seguir adiciona dois domínios confiáveis (cifs1.example.com e cifs2.example.com) à lista de domínios confiáveis preferida usada pelo SVM VS1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

O comando a seguir remove dois domínios confiáveis da lista usada pelo SVM VS1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

O comando a seguir modifica a lista de domínio confiável usada pelo SVM VS1. A nova lista substitui a lista original:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informações relacionadas

Exibindo informações sobre a lista de domínio confiável preferencial

Exibir informações sobre a lista de domínios confiáveis preferencial

Você pode exibir informações sobre quais domínios confiáveis estão na lista de domínios confiáveis preferenciais e a ordem em que eles são pesquisados se as pesquisas de mapeamento de nomes de vários domínios estiverem ativadas. Você pode configurar uma lista de domínio confiável preferida como alternativa ao uso da lista de domínio confiável descoberta automaticamente.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre o seguinte…	Use o comando…
Todos os domínios confiáveis preferenciais no cluster agrupados por máquina virtual de armazenamento (SVM)	`vserver cifs domain name-mapping-search show`
Todos os domínios confiáveis preferenciais para um SVM especificado	`vserver cifs domain name-mapping-search show -vserver` *vserver_name*

O comando a seguir exibe informações sobre todos os domínios confiáveis preferenciais no cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Informações relacionadas

Adicionar, remover ou substituir domínios confiáveis em listas de domínios confiáveis preferenciais

Crie e configure compartilhamentos SMB

Crie e configure a visão geral de compartilhamentos SMB

Para que usuários e aplicativos possam acessar dados no servidor CIFS em SMB, você deve criar e configurar compartilhamentos SMB, que é um ponto de acesso nomeado em um volume. Você pode personalizar compartilhamentos especificando parâmetros de compartilhamento e propriedades de compartilhamento. Você pode modificar um compartilhamento existente a qualquer momento.

Quando você cria um compartilhamento SMB, o ONTAP cria uma ACL padrão para as permissões de compartilhamento com controle total para todos.

Os compartilhamentos SMB estão vinculados ao servidor CIFS na máquina virtual de storage (SVM). Os compartilhamentos de SMB serão excluídos se o SVM for excluído ou se o servidor CIFS ao qual ele está associado for excluído do SVM. Se você recriar o servidor CIFS na SVM, será necessário recriar os compartilhamentos SMB.

Informações relacionadas

Gerencie o acesso a arquivos usando SMB

"Configuração SMB para Microsoft Hyper-V e SQL Server"

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Quais são os compartilhamentos administrativos padrão

Quando você cria um servidor CIFS na máquina virtual de storage (SVM), os compartilhamentos administrativos padrão são criados automaticamente. Você deve entender o que são esses compartilhamentos padrão e como eles são usados.

O ONTAP cria os seguintes compartilhamentos administrativos padrão quando você cria o servidor CIFS:

> A partir do ONTAP 9.8, o compartilhamento admin não é mais criado por padrão.

- ipc
- (Somente ONTAP 9.7 e versões anteriores)
- c

Como os compartilhamentos que terminam com o caractere dólar são compartilhamentos ocultos, os compartilhamentos administrativos padrão não são visíveis em meu computador, mas você pode visualizá-los usando pastas compartilhadas.

Como os compartilhamentos padrão do ipc e do admin são usados

As ações do ONTAP são usadas pelos administradores do Windows e não podem ser usadas pelos administradores do Windows para acessar dados residentes no SVM.

- compartilhar

  A ação ipc é um recurso que compartilha os pipes nomeados que são essenciais para a comunicação entre programas. O compartilhamento ipc é usado durante a administração remota de um computador e ao visualizar os recursos compartilhados de um computador. Não é possível alterar as configurações de compartilhamento, propriedades de compartilhamento ou ACLs do compartilhamento ipc. Você também não pode renomear ou excluir o compartilhamento ipc.

- Compartilhar (somente ONTAP 9.7 e anteriores)

  > A partir do ONTAP 9.8, o compartilhamento admin não é mais criado por padrão.

  O compartilhamento admin é usado durante a administração remota do SVM. O caminho desse recurso é sempre o caminho para a raiz do SVM. Você não pode alterar as configurações de compartilhamento, propriedades de compartilhamento ou ACLs para o compartilhamento admin. Você também não pode renomear ou excluir o compartilhamento admin.

Como o compartilhamento padrão c

O compartilhamento de CAD é um compartilhamento administrativo que o cluster ou o administrador do SVM pode usar para acessar e gerenciar o volume raiz do SVM.

A seguir estão as caraterísticas da participação:

- O caminho para esse compartilhamento é sempre o caminho para o volume raiz da SVM e não pode ser modificado.
- A ACL padrão para o compartilhamento c

  Este utilizador é o administrador. Por padrão, o administrador do BUILTIN pode mapear para o compartilhamento e exibição, criar, modificar ou excluir arquivos e pastas no diretório raiz mapeado. Cuidado deve ser exercido ao gerenciar arquivos e pastas neste diretório.
- Você pode alterar a ACL do compartilhamento.
- Você pode alterar as configurações de compartilhamento e as propriedades de compartilhamento.
- Não é possível eliminar a partilha c
- O administrador do SVM pode acessar o restante do namespace SVM a partir do compartilhamento mapeado por meio do cruzamento das junções do namespace.
- O compartilhamento c pode ser acessado usando o Console de Gerenciamento da Microsoft.

Informações relacionadas

Configurando permissões avançadas de arquivos NTFS usando a guia Segurança do Windows

Requisitos de nomenclatura para compartilhamento de SMB

Você deve manter os requisitos de nomenclatura do compartilhamento do ONTAP em mente ao criar compartilhamentos SMB no seu servidor SMB.

As convenções de nomes de compartilhamento para ONTAP são as mesmas que para o Windows e incluem os seguintes requisitos:

- O nome de cada compartilhamento deve ser exclusivo para o servidor SMB.
- Nomes de compartilhamento não diferenciam maiúsculas de minúsculas.
- O comprimento máximo do nome da partilha é de 80 carateres.
- Nomes de compartilhamento Unicode são suportados.
- Nomes de compartilhamento que terminam com o caractere dólar são compartilhamentos ocultos.
- Para o ONTAP 9.7 e anteriores, os compartilhamentos administrativos são criados automaticamente em todos os servidores CIFS e são nomes de compartilhamento reservados. A partir do ONTAP 9.8, o compartilhamento admin não é mais criado automaticamente.
- Você não pode usar o nome de compartilhamento ONTAP_ADMIN ao criar um compartilhamento.
- Nomes de compartilhamento que contêm espaços são suportados:
  - Você não pode usar um espaço como o primeiro caractere ou como o último caractere em um nome de compartilhamento.
  - Você deve incluir nomes de compartilhamento contendo um espaço entre aspas.

    As aspas simples são consideradas parte do nome da partilha e não podem ser utilizadas no lugar das aspas.
- Os seguintes carateres especiais são suportados quando você nomeia compartilhamentos SMB:

! A % e ' _ - . Clique em "OK"

- Os seguintes carateres especiais não são suportados quando você nomeia compartilhamentos SMB:
  - " / : ; | > , ? *

Requisitos de sensibilidade de caso de diretório ao criar compartilhamentos em um ambiente multiprotocolo

Se você criar compartilhamentos em um SVM em que o esquema de nomenclatura 8,3 seja usado para distinguir entre nomes de diretórios onde haja apenas diferenças de casos entre os nomes, você deve usar o nome 8,3 no caminho de compartilhamento para garantir que o cliente se conete ao caminho de diretório desejado.

No exemplo a seguir, dois diretórios chamados "testdir" e "TESTDIR" foram criados em um cliente Linux. O caminho de junção do volume que contém os diretórios é `/home`. A primeira saída é de um cliente Linux e a segunda saída é de um cliente SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Ao criar um compartilhamento no segundo diretório, você deve usar o nome 8,3 no caminho de compartilhamento. Neste exemplo, o caminho de compartilhamento para o primeiro diretório é `/home/testdir` e o caminho de compartilhamento para o segundo diretório é `/home/TESTDI~1`.

Use propriedades de compartilhamento SMB

Use a visão geral das propriedades de compartilhamento SMB

Você pode personalizar as propriedades dos compartilhamentos SMB.

As propriedades de compartilhamento disponíveis são as seguintes:

Compartilhar propriedades	Descrição
`oplocks`	Esta propriedade especifica que o compartilhamento usa bloqueios oportunistas, também conhecidos como cache do lado do cliente.
`browsable`	Esta propriedade permite que os clientes Windows naveguem na partilha.

Compartilhar propriedades	Descrição
`showsnapshot`	Essa propriedade especifica que as cópias Snapshot podem ser visualizadas e atravessadas por clientes.
`changenotify`	Esta propriedade especifica que o compartilhamento suporta solicitações Change Notify. Para compartilhamentos em um SVM, esta é uma propriedade inicial padrão.
`attributecache`	Essa propriedade permite que o cache de atributos de arquivo no compartilhamento SMB forneça acesso mais rápido aos atributos. O padrão é desabilitar o cache de atributos. Esta propriedade só deve ser ativada se houver clientes conetando-se a compartilhamentos sobre SMB 1,0. Essa propriedade de compartilhamento não se aplica se os clientes estiverem se conetando a compartilhamentos em SMB 2.x ou SMB 3,0.
`continuously-available`	Esta propriedade permite que clientes SMB que a suportam para abrir arquivos de forma persistente. Os arquivos abertos desta maneira são protegidos contra eventos disruptivos, como failover e giveback.
`branchcache`	Esta propriedade especifica que o compartilhamento permite que os clientes solicitem hashes BranchCache nos arquivos desse compartilhamento. Esta opção é útil somente se você especificar "'per-share'" como o modo operacional na configuração do CIFS BranchCache.
`access-based-enumeration`	Esta propriedade especifica que *Access Based Enumeração* (ABE) está ativada neste compartilhamento. As pastas compartilhadas filtradas por ABE são visíveis para um usuário com base nos direitos de acesso desse usuário individual, impedindo a exibição de pastas ou outros recursos compartilhados que o usuário não tem direitos de acesso.

Compartilhar propriedades	Descrição
`namespace-caching`	Esta propriedade especifica que os clientes SMB que se conetam a esse compartilhamento podem armazenar em cache os resultados da enumeração de diretórios retornados pelos servidores CIFS, o que pode fornecer melhor desempenho. Por padrão, os clientes SMB 1 não armazenam em cache os resultados da enumeração de diretórios. Como os clientes SMB 2 e SMB 3 armazenam resultados de enumeração de diretório em cache por padrão, especificar essa propriedade de compartilhamento fornece benefícios de desempenho apenas para conexões de cliente SMB 1.
`encrypt-data`	Esta propriedade especifica que a criptografia SMB deve ser usada ao acessar esse compartilhamento. Os clientes SMB que não suportam encriptação ao aceder a dados SMB não poderão aceder a esta partilha.

Adicione ou remova propriedades de compartilhamento em um compartilhamento SMB existente

Você pode personalizar um compartilhamento SMB existente adicionando ou removendo propriedades de compartilhamento. Isso pode ser útil se você quiser alterar a configuração de compartilhamento para atender às mudanças nos requisitos do seu ambiente.

Antes de começar

O compartilhamento cujas propriedades você deseja modificar deve existir.

Sobre esta tarefa

Diretrizes para adicionar propriedades de compartilhamento:

- Você pode adicionar uma ou mais propriedades de compartilhamento usando uma lista delimitada por vírgulas.
- Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.

  As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento.
- Se você especificar um novo valor para as propriedades de compartilhamento que já são aplicadas ao compartilhamento, o valor recém-especificado substituirá o valor original.
- Não é possível remover propriedades de compartilhamento usando o `vserver cifs share properties add` comando.

  Você pode usar o `vserver cifs share properties remove` comando para remover propriedades de compartilhamento.

Diretrizes para remover propriedades de compartilhamento:

- Você pode remover uma ou mais propriedades de compartilhamento usando uma lista delimitada por vírgulas.
- Todas as propriedades de compartilhamento que você especificou anteriormente, mas não as removem, permanecem em vigor.

Passos

1. Introduza o comando adequado:

Se você quiser…	Digite o comando…
Adicione propriedades de compartilhamento	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Remover propriedades de compartilhamento	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Verifique as configurações da propriedade de compartilhamento: `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemplos

O comando a seguir adiciona a `showsnapshot` propriedade share a uma ação chamada "hare1" no SVM VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

O comando a seguir remove a `browsable` propriedade share de um compartilhamento chamado "hare2" no SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Informações relacionadas

Comandos para gerenciar compartilhamentos SMB

Otimize o acesso do usuário SMB com a configuração de compartilhamento de grupo de força

Quando você cria um compartilhamento da linha de comando ONTAP para dados com segurança efetiva UNIX, você pode especificar que todos os arquivos criados por usuários SMB nesse compartilhamento pertencem ao mesmo grupo, conhecido como *force-group*, que deve ser um grupo predefinido no banco de dados de grupos UNIX. O uso de um grupo de força torna mais fácil garantir que os arquivos possam ser acessados por usuários SMB pertencentes a vários grupos.

Especificar um grupo de força é significativo apenas se o compartilhamento estiver em um UNIX ou em uma qtree misto. Não há necessidade de definir um grupo de força para compartilhamentos em um volume NTFS ou qtree porque o acesso a arquivos nesses compartilhamentos é determinado pelas permissões do Windows, não GIDs UNIX.

Se um grupo de força tiver sido especificado para uma ação, o seguinte se tornará verdadeiro para a partilha:

- Os usuários SMB no grupo de força que acessam esse compartilhamento são temporariamente alterados para o GID do grupo de força.

  Este GID permite que eles acessem arquivos neste compartilhamento que não são acessíveis normalmente com seu GID principal ou UID.

- Todos os arquivos neste compartilhamento criados por usuários SMB pertencem ao mesmo grupo de força, independentemente do GID principal do proprietário do arquivo.

Quando os usuários SMB tentam acessar um arquivo criado pelo NFS, os GIDs principais dos usuários SMB determinam os direitos de acesso.

O grupo force não afeta a forma como os usuários NFS acessam arquivos neste compartilhamento. Um arquivo criado por NFS adquire o GID do proprietário do arquivo. A determinação das permissões de acesso é baseada no UID e GID principal do usuário NFS que está tentando acessar o arquivo.

O uso de um grupo de força torna mais fácil garantir que os arquivos possam ser acessados por usuários SMB pertencentes a vários grupos. Por exemplo, se você quiser criar um compartilhamento para armazenar as páginas da Web da empresa e dar acesso de gravação a usuários nos departamentos de Engenharia e Marketing, você pode criar um compartilhamento e dar acesso de gravação a um grupo de força chamado "'webgroup1". Devido ao grupo force, todos os arquivos criados por usuários SMB neste compartilhamento

são de propriedade do grupo "'webgroup1". Além disso, os usuários recebem automaticamente o GID do grupo "'webgroup1" ao acessar o compartilhamento. Como resultado, todos os usuários podem escrever para esse compartilhamento sem que você precise gerenciar os direitos de acesso dos usuários nos departamentos de Engenharia e Marketing.

Informações relacionadas

Criando um compartilhamento SMB com a configuração de compartilhamento de grupo de força

Crie um compartilhamento SMB com a configuração de compartilhamento de grupo de força

Você pode criar um compartilhamento SMB com a configuração de compartilhamento de grupo de força se desejar que os usuários de SMB que acessam dados em volumes ou qtrees com segurança de arquivos UNIX sejam considerados pelo ONTAP como pertencentes ao mesmo grupo UNIX.

Passo

1. Crie o compartilhamento SMB: `vserver cifs share create -vserver` *`vserver_name`* `-share -name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Se o caminho UNC (`\\servername\sharename\filepath`) do compartilhamento contiver mais de 256 carateres (excluindo o " " " inicial`\\` no caminho UNC), a guia **Segurança** na caixa Propriedades do Windows não estará disponível. Este é um problema de cliente do Windows em vez de um problema de ONTAP. Para evitar esse problema, não crie compartilhamentos com caminhos UNC com mais de 256 carateres.

   Se você quiser remover o grupo de força depois que o compartilhamento é criado, você pode modificar o compartilhamento a qualquer momento e especificar uma string vazia ("") como o valor para o `-force -group-for-create` parâmetro. Se você remover o grupo de força modificando o compartilhamento, todas as conexões existentes a esse compartilhamento continuarão tendo o grupo de força definido anteriormente como GID principal.

Exemplo

O comando a seguir cria um compartilhamento "webpages" que é acessível na Web no `/corp/companyinfo` diretório no qual todos os arquivos criados pelos usuários SMB são atribuídos ao grupo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Informações relacionadas

Otimize o acesso do usuário SMB com a configuração de compartilhamento de grupo de força

Exibir informações sobre compartilhamentos SMB usando o MMC

Você pode exibir informações sobre compartilhamentos SMB no SVM e executar algumas tarefas de gerenciamento usando o Console de Gerenciamento da Microsoft (MMC). Antes de poder visualizar os compartilhamentos, você precisa conetar o MMC ao SVM.

Sobre esta tarefa

Você pode executar as seguintes tarefas em compartilhamentos contidos em SVMs usando o MMC:

- Ver compartilhamentos
- Ver sessões ativas
- Exibir arquivos abertos
- Enumerar a lista de sessões, ficheiros e ligações em árvore no sistema
- Feche os ficheiros abertos no sistema
- Feche as sessões abertas
- Criar/gerenciar compartilhamentos

> As visualizações exibidas pelos recursos anteriores são específicas de nós e não específicas de cluster. Portanto, quando você usa o MMC para se conetar ao nome do host do servidor SMB (ou seja, cifs01.domain.local), você é encaminhado, com base em como configurou o DNS, para um único LIF dentro do cluster.

As seguintes funções não são suportadas no MMC para ONTAP:

- Criando novos usuários/grupos locais
- Gerir/visualizar utilizadores/grupos locais existentes
- Visualização de eventos ou registos de desempenho
- Armazenamento
- Serviços e aplicações

Nos casos em que a operação não é suportada, você pode ter `remote procedure call failed` erros.

"Perguntas frequentes: Usando o Windows MMC com ONTAP"

Passos

1. Para abrir o MMC de Gerenciamento de computador em qualquer servidor Windows, no **Painel de Controle**, selecione **Ferramentas administrativas** > **Gerenciamento de computador**.
2. Selecione **Ação** > **ligar a outro computador**.

   A caixa de diálogo Selecionar computador é exibida.
3. Digite o nome do sistema de armazenamento ou clique em **Procurar** para localizar o sistema de armazenamento.
4. Clique em **OK**.

   O MMC se coneta ao SVM.
5. No painel de navegação, clique em **pastas compartilhadas** > **compartilhamentos**.

   Uma lista de compartilhamentos no SVM é exibida no painel de exibição direito.
6. Para exibir as propriedades de compartilhamento de um compartilhamento, clique duas vezes no compartilhamento para abrir a caixa de diálogo **Propriedades**.
7. Se você não puder se conetar ao sistema de armazenamento usando o MMC, você poderá adicionar o usuário ao grupo BUILTIN ou BUILTIN/Power Users usando um dos seguintes comandos no sistema de armazenamento:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Comandos para gerenciar compartilhamentos SMB

Use os `vserver cifs share` comandos e `vserver cifs share properties` para gerenciar compartilhamentos SMB.

Se você quiser…	Use este comando…
Crie um compartilhamento SMB	`vserver cifs share create`
Exibir compartilhamentos SMB	`vserver cifs share show`
Modificar um compartilhamento SMB	`vserver cifs share modify`
Excluir um compartilhamento SMB	`vserver cifs share delete`
Adicione propriedades de compartilhamento a um compartilhamento existente	`vserver cifs share properties add`
Remover propriedades de compartilhamento de um compartilhamento existente	`vserver cifs share properties remove`
Exibir informações sobre as propriedades de compartilhamento	`vserver cifs share properties show`

Consulte a página de manual de cada comando para obter mais informações.

Proteja o acesso a arquivos usando ACLs de compartilhamento SMB

Diretrizes para gerenciar ACLs de nível de compartilhamento SMB

Você pode alterar ACLs de nível de compartilhamento para dar aos usuários mais ou menos direitos de acesso ao compartilhamento. Você pode configurar ACLs de nível de compartilhamento usando usuários e grupos do Windows ou usuários e grupos UNIX.

Por padrão, a ACL de nível de compartilhamento dá controle total ao grupo padrão chamado Everyone. Controle total na ACL significa que todos os usuários no domínio e todos os domínios confiáveis têm acesso total ao compartilhamento. Você pode controlar o nível de acesso de uma ACL de nível de compartilhamento usando o "Console de Gerenciamento Microsoft (MMC) em um cliente Windows ou na linha de comando ONTAP".

As diretrizes a seguir se aplicam quando você usa o MMC:

- Os nomes de usuário e grupo especificados devem ser nomes do Windows.
- Você pode especificar apenas permissões do Windows.

As diretrizes a seguir se aplicam quando você usa a linha de comando ONTAP:

- Os nomes de usuário e grupo especificados podem ser nomes do Windows ou nomes UNIX.

  Se um tipo de usuário e grupo não for especificado ao criar ou modificar ACLs, o tipo padrão será usuários e grupos do Windows.

- Você pode especificar apenas permissões do Windows.

Criar listas de controle de acesso de compartilhamento SMB

A configuração de permissões de compartilhamento criando listas de controle de acesso (ACLs) para compartilhamentos SMB permite controlar o nível de acesso a um compartilhamento para usuários e grupos.

Sobre esta tarefa

Você pode configurar ACLs de nível de compartilhamento usando nomes de usuário ou grupo do Windows locais ou de domínio ou nomes de usuário ou grupo UNIX.

Antes de criar uma nova ACL, você deve excluir a ACL de compartilhamento padrão `Everyone / Full Control` , que representa um risco de segurança.

No modo de grupo de trabalho, o nome de domínio local é o nome do servidor SMB.

Passos

1. Exclua a ACL de compartilhamento padrão: 'Vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group everyone'
2. Configure a nova ACL:

Se você quiser configurar ACLs usando um…	Digite o comando…
Usuário do Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Grupo Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Se você quiser configurar ACLs usando um…	Digite o comando…
Utilizador UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Grupo UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Verifique se a ACL aplicada ao compartilhamento está correta usando o `vserver cifs share access-control show` comando.

Exemplo

O comando a seguir `Change` concede permissões ao grupo Windows "'equipe de vendas'" para o compartilhamento "vendas" no vs1.example.com.º SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

O comando a seguir `Read` dá permissão ao grupo UNIX "Engineering" para o compartilhamento "eng" no SVM "vs2.example.com":

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

Os comandos a seguir `Change` dão permissão ao grupo local do Windows chamado "Tiger Team" e `Full_Control` permissão ao usuário local do Windows chamado "Sue Chang" para o compartilhamento "datavol5" no SVM "VS1":

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Comandos para gerenciar listas de controle de acesso de compartilhamento SMB

Você precisa saber os comandos para gerenciar listas de controle de acesso (ACLs) SMB, o que inclui criar, exibir, modificar e excluir.

Se você quiser…	Use este comando…
Crie uma nova ACL	`vserver cifs share access-control create`
Exibir ACLs	`vserver cifs share access-control show`
Modificar uma ACL	`vserver cifs share access-control modify`
Eliminar uma ACL	`vserver cifs share access-control delete`

Proteja o acesso aos arquivos usando permissões de arquivo

Configure permissões avançadas de arquivos NTFS usando a guia Segurança do Windows

Você pode configurar permissões de arquivo NTFS padrão em arquivos e pastas usando a guia **Segurança do Windows** na janela Propriedades do Windows.

Antes de começar

O administrador que executa esta tarefa deve ter permissões NTFS suficientes para alterar permissões nos objetos selecionados.

Sobre esta tarefa

A configuração de permissões de arquivos NTFS é feita em um host do Windows adicionando entradas a listas de controle de acesso discricionárias (DACLs) NTFS associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS. Essas tarefas são tratadas automaticamente pela GUI do Windows.

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa de diálogo **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o nome do servidor CIFS que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

   Se o nome do servidor CIFS for "'CIFS_SERVER'" e o compartilhamento for chamado "hare1", você deverá digitar `\\CIFS_SERVER\share1`.

   > Você pode especificar o endereço IP da interface de dados para o servidor CIFS em vez do nome do servidor CIFS.

   c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

3. Selecione o arquivo ou diretório para o qual você deseja definir permissões de arquivo NTFS.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.

   A guia **Segurança** exibe a lista de usuários e grupos para os quais a permissão NTFS está definida. A caixa **Permissions for** exibe uma lista de permissões de permissão e negação em vigor para cada usuário ou grupo selecionado.

6. Clique em **Avançado**.

   A janela Propriedades do Windows exibe informações sobre permissões de arquivo existentes atribuídas a usuários e grupos.

7. Clique em **alterar permissões**.

   A janela permissões é aberta.

8. Execute as ações desejadas:

Se você quiser…	Faça o seguinte…
Configurar permissões NTFS avançadas para um novo utilizador ou grupo	a. Clique em **Add**. b. Na caixa **Digite o nome do objeto a ser selecionado**, digite o nome do usuário ou grupo que deseja adicionar. c. Clique em **OK**.
Alterar permissões NTFS avançadas de um usuário ou grupo	a. Na caixa **entradas de permissões:**, selecione o usuário ou grupo cujas permissões avançadas você deseja alterar. b. Clique em **Editar**.
Remover permissões NTFS avançadas para um usuário ou grupo	a. Na caixa **entradas de permissões:**, selecione o usuário ou grupo que deseja remover. b. Clique em **Remover**. c. Avance para o passo 13.

   Se você estiver adicionando permissões NTFS avançadas em um novo usuário ou grupo ou alterando permissões avançadas NTFS em um usuário ou grupo existente, a caixa Entrada de permissão para <Object> será aberta.

9. Na caixa **Apply to**, selecione como você deseja aplicar esta entrada de permissão de arquivo NTFS.

   Se você estiver configurando permissões de arquivo NTFS em um único arquivo, a caixa **Apply to** não estará ativa. A configuração **apply to** é padrão para **this object only**.

10. Na caixa **Permissions**, selecione as caixas **allow** ou **deny** para as permissões avançadas que você deseja definir neste objeto.

    ◦ Para permitir o acesso especificado, selecione a caixa **permitir**.

- Para não permitir o acesso especificado, selecione a caixa **Negar**. Você pode definir permissões nos seguintes direitos avançados:
- * Controle total*

  Se você escolher esse direito avançado, todos os outros direitos avançados serão escolhidos automaticamente (permitir ou negar direitos).

- * Traverse pasta / executar arquivo *
- **Lista de pastas / dados de leitura**
- **Leia atributos**
- **Leia atributos estendidos**
- * Criar arquivos / escrever dados *
- * Criar pastas / anexar dados*
- * Escrever atributos*
- **Escreva atributos estendidos**
- **Excluir subpastas e arquivos**
- **Excluir**
- **Permissões de leitura**
- **Alterar permissões**
- **Assuma a propriedade**

  Se qualquer uma das caixas de permissão avançada não for selecionável, é porque as permissões são herdadas do objeto pai.

11. Se você quiser que subpastas e arquivos desse objeto herdem essas permissões, marque a caixa **aplicar essas permissões a objetos e/ou contentores dentro desse contentor somente**.
12. Clique em **OK**.
13. Depois de terminar de adicionar, remover ou editar permissões NTFS, especifique a configuração de herança para este objeto:

    - Selecione a caixa **incluir permissões herdadas a partir da caixa pai** deste objeto.

      Este é o padrão.

    - Selecione a caixa **Substituir todas as permissões de objeto filho por permissões herdadas deste objeto**.

      Esta configuração não está presente na caixa permissões se você estiver definindo permissões de arquivo NTFS em um único arquivo.

Tenha cuidado ao selecionar esta definição. Esta configuração remove todas as permissões existentes em todos os objetos filho e as substitui pelas configurações de permissão deste objeto. Você pode remover inadvertidamente as permissões que você não queria que fossem removidas. É especialmente importante ao definir permissões em um volume ou qtree misto de estilo de segurança. Se objetos filho tiverem um estilo de segurança eficaz UNIX, propagar permissões NTFS para esses objetos filho resulta na alteração do ONTAP desses objetos do estilo de segurança UNIX para o estilo de segurança NTFS e todas as permissões UNIX nesses objetos filho serão substituídas por permissões NTFS.

- Selecione ambas as caixas.
- Selecione nenhuma das caixas.

14. Clique em **OK** para fechar a caixa **permissões**.
15. Clique em **OK** para fechar a caixa **Configurações avançadas de segurança para o <Object>**.

Para obter mais informações sobre como definir permissões NTFS avançadas, consulte a documentação do Windows.

Informações relacionadas

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Configurar permissões de arquivos NTFS usando a CLI do ONTAP

Você pode configurar permissões de arquivos NTFS em arquivos e diretórios usando a CLI do ONTAP. Isso permite configurar permissões de arquivos NTFS sem precisar se conetar aos dados usando um compartilhamento SMB em um cliente Windows.

Você pode configurar permissões de arquivo NTFS adicionando entradas a listas de controle de acesso discricionário NTFS (DACLs) associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS.

Você só pode configurar permissões de arquivo NTFS usando a linha de comando. Você não pode configurar ACLs NFSv4 usando a CLI.

Passos

1. Crie um descritor de segurança NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Adicione DACLs ao descritor de segurança NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
```

```
{this-folder|sub-folders|files}
```

3. Crie uma política de segurança de arquivo/diretório.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

Como as permissões de arquivo UNIX fornecem controle de acesso ao acessar arquivos por SMB

Um FlexVol volume pode ter um dos três tipos de estilo de segurança: NTFS, UNIX ou misto. Você pode acessar dados sobre SMB independentemente do estilo de segurança; no entanto, permissões de arquivo UNIX apropriadas são necessárias para acessar dados com segurança efetiva UNIX.

Quando os dados são acessados por SMB, há vários controles de acesso usados para determinar se um usuário está autorizado a executar uma ação solicitada:

- Permissões de exportação

  Configurar permissões de exportação para o acesso SMB é opcional.

- Permissões de compartilhamento
- Permissões de arquivo

  Os seguintes tipos de permissões de arquivo podem ser aplicados aos dados nos quais o usuário deseja executar uma ação:

  - NTFS
  - ACLs do UNIX NFSv4
  - Bits do modo UNIX

Para dados com ACLs NFSv4 ou bits de modo UNIX definidos, as permissões de estilo UNIX são usadas para determinar os direitos de acesso aos dados. O administrador do SVM precisa definir a permissão de arquivo apropriada para garantir que os usuários tenham os direitos para executar a ação desejada.

Os dados em um volume misto de estilo de segurança podem ter um estilo de segurança eficaz NTFS ou UNIX. Se os dados tiverem um estilo de segurança eficaz UNIX, as permissões NFSv4 ou os bits de modo UNIX serão usados ao determinar os direitos de acesso aos dados.

Acesso seguro a arquivos usando o controle de acesso dinâmico (DAC)

Proteja o acesso a ficheiros utilizando a visão geral do controlo de acesso dinâmico (DAC)

Você pode proteger o acesso usando o Controle de Acesso Dinâmico e criando políticas de acesso centrais no ative Directory e aplicando-as a arquivos e pastas em SVMs por meio de objetos de Diretiva de Grupo aplicados (GPOs). Você pode configurar a auditoria para usar eventos de preparação de políticas de acesso central para ver os efeitos das alterações nas políticas de acesso central antes de aplicá-las.

Adições às credenciais CIFS

Antes do Controle de Acesso Dinâmico, uma credencial CIFS incluía a identidade de um responsável de segurança (o usuário) e a associação de grupo do Windows. Com o Dynamic Access Control, mais três tipos de informações são adicionados à identidade do dispositivo, às declarações do dispositivo e às declarações do usuário:

- Identidade do dispositivo

  O analógico das informações de identidade do usuário, exceto se for a identidade e associação de grupo do dispositivo do qual o usuário está fazendo login.

- Reclamações do dispositivo

  Afirmações sobre um dispositivo principal de segurança. Por exemplo, uma alegação de dispositivo pode ser que ela seja membro de uma ou específica.

- Reclamações do utilizador

  Afirmações sobre um responsável de segurança do usuário. Por exemplo, uma alegação de usuário pode ser que sua conta do AD seja membro de uma ou específica.

Políticas de acesso central

As políticas de acesso central para arquivos permitem que as organizações implantem e gerenciem centralmente políticas de autorização que incluem expressões condicionais usando grupos de usuários, reivindicações de usuários, declarações de dispositivos e propriedades de recursos.

Por exemplo, para acessar dados de alto impactos nos negócios, um usuário precisa ser um funcionário em tempo integral e ter acesso apenas aos dados de um dispositivo gerenciado. As políticas de acesso central são definidas no ative Directory e distribuídas para servidores de arquivos através do mecanismo GPO.

Preparação de políticas de acesso central com auditoria avançada

As políticas de acesso central podem ser "envelhecidas", caso em que são avaliadas de forma "'What-if'" durante as verificações de acesso ao arquivo. Os resultados do que teria acontecido se a política estivesse em vigor e como isso difere do que está configurado atualmente são registrados como um evento de auditoria. Dessa forma, os administradores podem usar logs de eventos de auditoria para estudar o impactos de uma alteração de política de acesso antes de realmente colocar a política em jogo. Depois de avaliar o impactos de uma alteração de política de acesso, a política pode ser implantada via GPOs nos SVMs desejados.

Informações relacionadas

GPOs compatíveis

Aplicando objetos de Diretiva de Grupo a servidores CIFS

Ativar ou desativar o suporte de GPO num servidor CIFS

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Exibindo informações sobre as regras da política de acesso central

Configuração de políticas de acesso central para proteger dados em servidores CIFS

Exibindo informações sobre a segurança do controle de acesso dinâmico

"Auditoria de SMB e NFS e rastreamento de segurança"

Funcionalidade de controlo de acesso dinâmico suportada

Se você quiser usar o controle de acesso dinâmico (DAC) em seu servidor CIFS, você precisa entender como o ONTAP suporta a funcionalidade de controle de acesso dinâmico em ambientes do ative Directory.

Suportado para controlo de acesso dinâmico

O ONTAP suporta a seguinte funcionalidade quando o controlo de acesso dinâmico está ativado no servidor CIFS:

Funcionalidade	Comentários
Reclamações no sistema de arquivos	Reivindicações são pares simples de nome e valor que afirmam alguma verdade sobre um usuário. As credenciais do usuário contêm informações de reclamação, e os descritores de segurança nos arquivos podem executar verificações de acesso que incluem verificações de reclamações. Isso dá aos administradores um nível mais alto de controle sobre quem pode acessar arquivos.
Expressões condicionais para verificações de acesso a arquivos	Ao modificar os parâmetros de segurança de um arquivo, os usuários podem adicionar expressões condicionais arbitrariamente complexas ao descritor de segurança do arquivo. A expressão condicional pode incluir verificações para reclamações.
Controle central do acesso a arquivos através de políticas de acesso central	As políticas de acesso central são um tipo de ACL armazenada no ative Directory que pode ser marcada para um arquivo. O acesso ao arquivo só é concedido se as verificações de acesso do descritor de segurança no disco e da diretiva de acesso central marcada permitirem o acesso. Isso dá aos administradores a capacidade de controlar o acesso a arquivos de um local central (AD) sem ter que modificar o descritor de segurança no disco.
Preparação da política de acesso central	Adiciona a capacidade de testar alterações de segurança sem afetar o acesso real aos arquivos, "definindo" uma alteração nas políticas de acesso central e vendo o efeito da alteração em um relatório de auditoria.
Suporte para exibir informações sobre a segurança da diretiva de acesso central usando a CLI do ONTAP	Estende o `vserver security file-directory show` comando para exibir informações sobre políticas de acesso centrais aplicadas.

Funcionalidade	Comentários
Rastreamento de segurança que inclui políticas de acesso central	Estende a `vserver security trace` família de comandos para exibir resultados que incluem informações sobre políticas de acesso central aplicadas.

Não suportado para o controlo de acesso dinâmico

O ONTAP não suporta a seguinte funcionalidade quando o controlo de acesso dinâmico está ativado no servidor CIFS:

Funcionalidade	Comentários
Classificação automática de objetos do sistema de arquivos NTFS	Esta é uma extensão para a infra-estrutura de classificação de ficheiros do Windows que não é suportada no ONTAP.
Auditoria avançada que não a preparação de políticas de acesso central	Somente o estadiamento da política de acesso central é suportado para auditoria avançada.

Considerações ao usar o Controle de Acesso Dinâmico e políticas de Acesso Central com servidores CIFS

Há certas considerações que você deve ter em mente ao usar o controle de acesso dinâmico (DAC) e as políticas de acesso central para proteger arquivos e pastas em servidores CIFS.

O acesso NFS pode ser negado ao root se a regra de política se aplicar ao usuário do domínio/administrador

Em determinadas circunstâncias, o acesso NFS à raiz pode ser negado quando a segurança da diretiva de acesso central é aplicada aos dados que o usuário raiz está tentando acessar. O problema ocorre quando a política de acesso central contém uma regra que é aplicada ao domínio/administrador e a conta raiz é mapeada para a conta de domínio/administrador.

Em vez de aplicar uma regra ao utilizador de domínio/administrador, deve aplicar a regra a um grupo com Privileges administrativo, como o grupo de domínio/administradores. Desta forma, pode mapear a raiz para a conta de domínio/administrador sem que a raiz seja afetada por este problema.

O grupo BUILTIN/Administradores do servidor CIFS tem acesso a recursos quando a diretiva de acesso central aplicado não é encontrada no ative Directory

É possível que os recursos contidos no servidor CIFS tenham políticas de acesso central aplicadas a eles, mas quando o servidor CIFS usa o SID da política de acesso central para tentar recuperar informações do ative Directory, o SID não corresponde a nenhum SIDs de política de acesso central existente no ative Directory. Nestas circunstâncias, o servidor CIFS aplica a política de recuperação padrão local para esse recurso.

A política de recuperação padrão local permite o acesso do grupo BUILTIN/Administradores do servidor CIFS a esse recurso.

Ativar ou desativar a descrição geral do controlo de Acesso Dinâmico

A opção que permite utilizar o controlo de Acesso Dinâmico (DAC) para proteger objetos no servidor CIFS está desativada por predefinição. Você deve ativar a opção se quiser usar o Controle de Acesso Dinâmico no servidor CIFS. Se decidir mais tarde que não pretende utilizar o controlo de Acesso Dinâmico para proteger objetos armazenados no servidor CIFS, pode desativar a opção.

Sobre esta tarefa

Uma vez que o Controle de Acesso Dinâmico esteja ativado, o sistema de arquivos pode conter ACLs com entradas relacionadas ao Controle de Acesso Dinâmico. Se o controlo de Acesso Dinâmico estiver desativado, as entradas atuais do controlo de Acesso Dinâmico serão ignoradas e as novas não serão permitidas.

Esta opção está disponível apenas no nível de privilégio avançado.

Passo

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que o Controle de Acesso Dinâmico seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Configuração de políticas de acesso central para proteger dados em servidores CIFS

Gerencie ACLs que contêm ACEs de controle de acesso dinâmico quando o controle de acesso dinâmico estiver desativado

Se você tiver recursos que têm ACLs aplicadas com ACEs de controle de acesso dinâmico e desativar o controle de acesso dinâmico na máquina virtual de armazenamento (SVM), remova os ACEs de controle de acesso dinâmico antes de gerenciar os ACEs de controle de acesso não dinâmico nesse recurso.

Sobre esta tarefa

Depois de o controlo de acesso dinâmico ser desativado, não é possível remover os ACEs de controlo de acesso não dinâmico existentes nem adicionar novos ACEs de controlo de acesso não dinâmico até ter removido os ACEs de controlo de acesso dinâmico existentes.

Você pode usar qualquer ferramenta usada normalmente para gerenciar ACLs para executar essas etapas.

Passos

1. Determine quais ACEs do controle de acesso dinâmico são aplicados ao recurso.
2. Remova os ACEs de controle de acesso dinâmico do recurso.
3. Adicione ou remova ACEs não-Dynamic Access Control conforme desejado do recurso.

Configurar políticas de acesso central para proteger dados em servidores CIFS

Há várias etapas que você deve seguir para proteger o acesso aos dados no servidor CIFS usando políticas de acesso central, incluindo habilitar o DAC (Dynamic Access Control) no servidor CIFS, configurar políticas de acesso central no ative Directory, aplicar as políticas de acesso central a contentores do ative Directory com GPOs e habilitar GPOs no servidor CIFS.

Antes de começar

- O ative Directory deve ser configurado para usar políticas de acesso central.
- Você precisa ter acesso suficiente nos controladores de domínio do ative Directory para criar políticas de acesso centrais e para criar e aplicar GPOs aos contêineres que contêm os servidores CIFS.
- Você precisa ter acesso administrativo suficiente na máquina virtual de storage (SVM) para executar os comandos necessários.

Sobre esta tarefa

As políticas de acesso central são definidas e aplicadas a objetos de diretiva de grupo (GPOs) no active Directory. Você pode consultar a Biblioteca Microsoft TechNet para obter instruções sobre como configurar políticas de acesso central e GPOs.

"Microsoft TechNet Library"

Passos

1. Ative o controle de acesso dinâmico na SVM se ele ainda não estiver habilitado usando o `vserver cifs options modify` comando.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Habilite os objetos de diretiva de grupo (GPOs) no servidor CIFS se eles ainda não estiverem habilitados usando o `vserver cifs group-policy modify` comando.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Crie regras de acesso central e políticas de acesso central no ative Directory.
4. Crie um objeto de diretiva de grupo (GPO) para implantar as políticas de acesso central no ative Directory.
5. Aplique o GPO ao recipiente onde a conta do computador do servidor CIFS está localizada.
6. Atualize manualmente os GPOs aplicados ao servidor CIFS usando o `vserver cifs group-policy update` comando.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Verifique se a diretiva de acesso central GPO é aplicada aos recursos no servidor CIFS usando o `vserver cifs group-policy show-applied` comando.

   O exemplo a seguir mostra que a Diretiva de domínio padrão tem duas diretivas de acesso central

aplicadas ao servidor CIFS:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
------------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
```

```
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Exibindo informações sobre as regras da política de acesso central

Ativar ou desativar o controlo de acesso dinâmico

Apresentar informações sobre a segurança do controlo de acesso dinâmico

Pode apresentar informações sobre a segurança do controlo de acesso dinâmico (DAC) em volumes NTFS e em dados com segurança eficaz NTFS em volumes mistos de estilo de segurança. Isso inclui informações sobre ACEs condicionais, ACEs de recursos e ACEs de política de acesso central. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Onde a saída é exibida com SIDs de grupo e usuário	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Sobre segurança de arquivos e diretórios para arquivos e diretórios onde a máscara de bits hexadecimal é traduzida para o formato textual	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Exemplos

O exemplo a seguir exibe informações de segurança do Dynamic Access Control sobre o caminho `/vol1` no SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Exibindo informações sobre as regras da política de acesso central

Considerações de reversão para o Controle de Acesso Dinâmico

Você deve estar ciente do que acontece ao reverter para uma versão do ONTAP que não suporta o controle de acesso dinâmico (DAC) e o que você deve fazer antes e depois de reverter.

Se você quiser reverter o cluster para uma versão do ONTAP que não suporte o Controle de Acesso Dinâmico e o Controle de Acesso Dinâmico estiver ativado em uma ou mais máquinas virtuais de armazenamento (SVMs), faça o seguinte antes de reverter:

- Você deve desativar o Controle de Acesso Dinâmico em todos os SVMs que o tenham ativado no cluster.
- É necessário modificar qualquer configuração de auditoria no cluster que contenha o `cap-staging` tipo de evento para usar somente o `file-op` tipo de evento.

Você deve entender e agir sobre algumas considerações importantes de reversão para arquivos e pastas com ACEs de Controle de Acesso Dinâmico:

- Se o cluster for revertido, os ACEs de Controle de Acesso Dinâmico existentes não serão removidos; no entanto, eles serão ignorados nas verificações de acesso ao arquivo.
- Uma vez que os ACEs do controlo de Acesso Dinâmico são ignorados após a reversão, o acesso aos ficheiros será alterado nos ficheiros com ACEs do controlo de Acesso Dinâmico.

  Isso poderia permitir que os usuários acessem arquivos que eles anteriormente não podiam, ou não poderiam acessar arquivos que anteriormente poderiam.

- Você deve aplicar ACEs não-Dynamic Access Control aos arquivos afetados para restaurar seu nível anterior de segurança.

  Isso pode ser feito antes de reverter ou imediatamente após a reversão ser concluída.

> Uma vez que os ACEs do controlo de Acesso Dinâmico são ignorados após a reversão, não é necessário removê-los ao aplicar ACEs do controlo de Acesso não Dinâmico aos ficheiros afetados. No entanto, se desejado, você pode removê-los manualmente.

Onde encontrar informações adicionais sobre como configurar e usar o Controle de Acesso Dinâmico e as políticas de Acesso Central

Recursos adicionais estão disponíveis para ajudá-lo a configurar e usar o controle de acesso dinâmico e as políticas de acesso central.

Você pode encontrar informações sobre como configurar o Controle de Acesso Dinâmico e as políticas de Acesso Central no ative Directory na Biblioteca Microsoft TechNet.

"Microsoft TechNet: Visão geral do cenário Dynamic Access Control"

"Microsoft TechNet: Cenário de Política de Acesso Central"

As referências a seguir podem ajudá-lo a configurar o servidor SMB para usar e dar suporte ao Controle de Acesso Dinâmico e às políticas de Acesso Central:

- **Usando GPOs no servidor SMB**

  Aplicando objetos de Diretiva de Grupo a servidores SMB

- **Configurando a auditoria nas no servidor SMB**

  "Auditoria de SMB e NFS e rastreamento de segurança"

Acesso SMB seguro usando políticas de exportação

Como as políticas de exportação são usadas com o acesso SMB

Se as políticas de exportação para acesso SMB estiverem habilitadas no servidor SMB, as políticas de exportação serão usadas ao controlar o acesso a volumes SVM por clientes SMB. Para acessar dados, você pode criar uma política de exportação que permita o acesso SMB e, em seguida, associá-la aos volumes que contêm compartilhamentos SMB.

Uma política de exportação tem uma ou mais regras aplicadas a ela que especifica quais clientes têm permissão de acesso aos dados e quais protocolos de autenticação são suportados para acesso somente leitura e gravação. Você pode configurar políticas de exportação para permitir o acesso por SMB a todos os clientes, uma sub-rede de clientes ou um cliente específico e para permitir a autenticação usando autenticação Kerberos, autenticação NTLM ou autenticação Kerberos e NTLM ao determinar o acesso somente leitura e gravação aos dados.

Depois de processar todas as regras de exportação aplicadas à política de exportação, o ONTAP pode determinar se o cliente recebe acesso e que nível de acesso é concedido. As regras de exportação se aplicam a máquinas cliente, não a usuários e grupos do Windows. As regras de exportação não substituem a autenticação e autorização baseadas em grupo e no utilizador do Windows. As regras de exportação fornecem outra camada de segurança de acesso, além das permissões de compartilhamento e acesso a arquivos.

Você associa exatamente uma política de exportação a cada volume para configurar o acesso do cliente ao volume. Cada SVM pode conter várias políticas de exportação. Isso permite que você faça o seguinte para SVMs com vários volumes:

- Atribua diferentes políticas de exportação a cada volume do SVM para controle de acesso de cliente individual a cada volume no SVM.
- Atribua a mesma política de exportação a vários volumes do SVM para controle de acesso de cliente idêntico sem precisar criar uma nova política de exportação para cada volume.

Cada SVM tem pelo menos uma política de exportação chamada "falha", que não contém regras. Não é possível excluir esta política de exportação, mas você pode renomeá-la ou modificá-la. Por padrão, cada volume no SVM está associado à política de exportação padrão. Se as políticas de exportação para acesso SMB estiverem desativadas no SVM, a política de exportação "falha" não terá efeito no acesso SMB.

Você pode configurar regras que fornecem acesso a hosts NFS e SMB e associar essa regra a uma política de exportação, que pode ser associada ao volume que contém dados ao qual hosts NFS e SMB precisam acessar. Alternativamente, se houver alguns volumes em que apenas clientes SMB exigem acesso, você poderá configurar uma política de exportação com regras que só permitem acesso usando o protocolo SMB e que usa apenas Kerberos ou NTLM (ou ambos) para autenticação para acesso somente leitura e gravação. A política de exportação é então associada aos volumes em que apenas o acesso SMB é desejado.

Se as políticas de exportação para SMB estiverem ativadas e um cliente fizer uma solicitação de acesso não permitida pela política de exportação aplicável, a solicitação falhará com uma mensagem de permissão negada. Se um cliente não corresponder a nenhuma regra na política de exportação do volume, o acesso será negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados. Isso é verdade mesmo se as permissões de compartilhamento e arquivo permitissem o acesso. Isso significa que você deve configurar sua política de exportação para permitir minimamente o seguinte em volumes que contêm compartilhamentos SMB:

- Permitir o acesso a todos os clientes ou ao subconjunto apropriado de clientes
- Permitir acesso através de SMB
- Permitir acesso apropriado somente leitura e gravação usando a autenticação Kerberos ou NTLM (ou ambas)

Saiba mais "configuração e gerenciamento de políticas de exportação"sobre .

Como funcionam as regras de exportação

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente a um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente.

Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação. A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

Você pode configurar regras de exportação para determinar permissões de acesso do cliente usando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação, por exemplo, NFSv4 ou SMB.
- Um identificador de cliente, por exemplo, nome de host ou endereço IP.

  O tamanho máximo para o `-clientmatch` campo é de 4096 carateres.

- O tipo de segurança usado pelo cliente para autenticar, por exemplo, Kerberos v5, NTLM ou AUTH_SYS.

Se uma regra especificar vários critérios, o cliente deve corresponder a todos eles para que a regra seja aplicada.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv3 e o cliente tem o endereço IP 10,1.17,37.

Mesmo que o protocolo de acesso do cliente corresponda, o endereço IP do cliente está em uma sub-rede diferente da especificada na regra de exportação. Portanto, a correspondência do cliente falha e esta regra não se aplica a este cliente.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv4 e o cliente tem o endereço IP 10,1.16,54.

O protocolo de acesso do cliente corresponde e o endereço IP do cliente está na sub-rede especificada. Portanto, a correspondência do cliente é bem-sucedida e esta regra se aplica a este cliente. O cliente obtém acesso de leitura e gravação independentemente do seu tipo de segurança.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. Portanto, ambos os clientes recebem acesso somente leitura. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

Exemplos de regras de política de exportação que restringem ou permitem acesso através de SMB

Os exemplos mostram como criar regras de política de exportação que restringem ou permitem o acesso ao SMB em um SVM que tenha políticas de exportação para acesso ao SMB ativadas.

As políticas de exportação para o acesso SMB estão desativadas por predefinição. Você precisa configurar regras de política de exportação que restrinjam ou permitam acesso ao SMB somente se você tiver ativado políticas de exportação para acesso ao SMB.

Regra de exportação apenas para acesso SMB

O comando a seguir cria uma regra de exportação no SVM chamado "'VS1" que tem a seguinte configuração:

- Nome da política: cifs1
- Número de índice: 1

- Correspondência de cliente: Corresponde apenas a clientes na rede 192.168.1.0/24
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Para clientes que usam autenticação NTLM ou Kerberos
- Acesso de leitura-gravação: Para clientes que usam a autenticação Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regra de exportação para SMB e acesso NFS

O comando a seguir cria uma regra de exportação no SVM chamado"' VS1" que tem a seguinte configuração:

- Nome da política: cifsnfs1
- Número de índice: 2
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Acesso SMB e NFS
- Acesso somente leitura: Para todos os clientes
- Acesso de leitura e gravação: Para clientes que usam Kerberos (NFS e SMB) ou autenticação NTLM (SMB)
- Mapeamento para ID de usuário UNIX 0 (zero): Mapeado para ID de usuário 65534 (que normalmente mapeia para o nome de usuário ninguém)
- Acesso suid e sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regra de exportação para acesso SMB usando apenas NTLM

O comando a seguir cria uma regra de exportação no SVM chamado "'VS1" que tem a seguinte configuração:

- Nome da política: ntlm1
- Número de índice: 1
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Somente para clientes que usam NTLM
- Acesso de leitura e gravação: Apenas para clientes que utilizam NTLM

Se você configurar a opção somente leitura ou a opção leitura-gravação para acesso somente NTLM, você deverá usar entradas baseadas em endereço IP na opção correspondência do cliente. Caso contrário, você recebe `access denied` erros. Isso ocorre porque o ONTAP usa os nomes principais do Serviço Kerberos (SPN) ao usar um nome de host para verificar os direitos de acesso do cliente. A autenticação NTLM não suporta nomes SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Ativar ou desativar políticas de exportação para acesso SMB

Você pode ativar ou desativar políticas de exportação para acesso SMB em máquinas virtuais de armazenamento (SVMs). O uso de políticas de exportação para controlar o acesso SMB a recursos é opcional.

Antes de começar

A seguir estão os requisitos para ativar políticas de exportação para SMB:

- O cliente deve ter um Registro "PTR" no DNS antes de criar as regras de exportação para esse cliente.
- Um conjunto adicional de Registros "'A'" e "'PTR'" para nomes de host é necessário se o SVM fornecer acesso a clientes NFS e o nome de host que você deseja usar para acesso NFS for diferente do nome do servidor CIFS.

Sobre esta tarefa

Ao configurar um novo servidor CIFS na SVM, o uso de políticas de exportação para acesso SMB é desativado por padrão. Você pode habilitar políticas de exportação para acesso SMB se quiser controlar o acesso com base no protocolo de autenticação ou em endereços IP de cliente ou nomes de host. Você pode ativar ou desativar políticas de exportação para acesso SMB a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ativar ou desativar políticas de exportação:
   - Ativar políticas de exportação: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - Desativar políticas de exportação: `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled false`
3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir permite o uso de políticas de exportação para controlar o acesso de clientes SMB a recursos no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Além de proteger o acesso usando a segurança nativa em nível de arquivo e exportar e compartilhar, você pode configurar o Storage-Level Access Guard, uma terceira camada de segurança aplicada pelo ONTAP no nível de volume. O Storage-Level Access Guard se aplica ao acesso de todos os protocolos nas ao objeto de storage ao qual ele é aplicado.

Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

Comportamento do Access Guard no nível de storage

- O Storage-Level Access Guard aplica-se a todos os arquivos ou a todos os diretórios em um objeto de armazenamento.

  Como todos os arquivos ou diretórios em um volume estão sujeitos às configurações do Storage-Level Access Guard, a herança através da propagação não é necessária.

- Você pode configurar o Storage-Level Access Guard para se aplicar apenas a arquivos, apenas a diretórios ou a arquivos e diretórios dentro de um volume.
  - Segurança de arquivos e diretórios

    Aplica-se a cada diretório e arquivo dentro do objeto de armazenamento. Esta é a configuração padrão.

  - Segurança de arquivos

    Aplica-se a todos os arquivos dentro do objeto de armazenamento. A aplicação dessa segurança não afeta o acesso ou a auditoria de diretórios.

  - Segurança do diretório

    Aplica-se a todos os diretórios dentro do objeto de armazenamento. A aplicação dessa segurança não afeta o acesso ou a auditoria de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

- Se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard.

  Ele é aplicado no nível do objeto de armazenamento e armazenado nos metadados usados para determinar as permissões efetivas.

- A segurança no nível do storage não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX).

  Ele foi desenvolvido para ser modificado apenas por administradores de storage.

- Você pode aplicar o Storage-Level Access Guard a volumes com NTFS ou estilo de segurança misto.
- Você pode aplicar o Storage-Level Access Guard a volumes com estilo de segurança UNIX, desde que o SVM que contém o volume tenha um servidor CIFS configurado.
- Quando os volumes são montados sob um caminho de junção de volume e se o Storage-Level Access Guard estiver presente nesse caminho, ele não será propagado para volumes montados sob ele.
- O descritor de segurança do Access Guard em nível de storage é replicado com a replicação de dados do SnapMirror e com replicação SVM.
- Há dispensação especial para scanners de vírus.

  Acesso excecional é permitido a esses servidores para exibir arquivos e diretórios, mesmo que o Storage-Level Access Guard negue acesso ao objeto.

- As notificações FPolicy não são enviadas se o acesso for negado devido ao Storage-Level Access Guard.

Verificações de ordem de acesso

O acesso a um arquivo ou diretório é determinado pelo efeito combinado das permissões de exportação ou compartilhamento, as permissões de guarda de acesso em nível de armazenamento definidas em volumes e as permissões de arquivo nativo aplicadas a arquivos e/ou diretórios. Todos os níveis de segurança são avaliados para determinar quais as permissões efetivas de um arquivo ou diretório. As verificações de acesso de segurança são realizadas na seguinte ordem:

1. Permissões de compartilhamento SMB ou nível de exportação NFS
2. Proteção de acesso no nível de storage
3. Listas de controle de acesso (ACLs) de arquivos/pastas NTFS, ACLs NFSv4 ou bits de modo UNIX

Casos de uso para usar o Storage-Level Access Guard

O Storage-Level Access Guard fornece segurança adicional no nível de armazenamento, que não é visível do lado do cliente; portanto, ele não pode ser revogado por nenhum dos usuários ou administradores de seus desktops. Há certos casos de uso em que a capacidade de controlar o acesso no nível de storage é benéfica.

Os casos de uso típicos para esse recurso incluem os seguintes cenários:

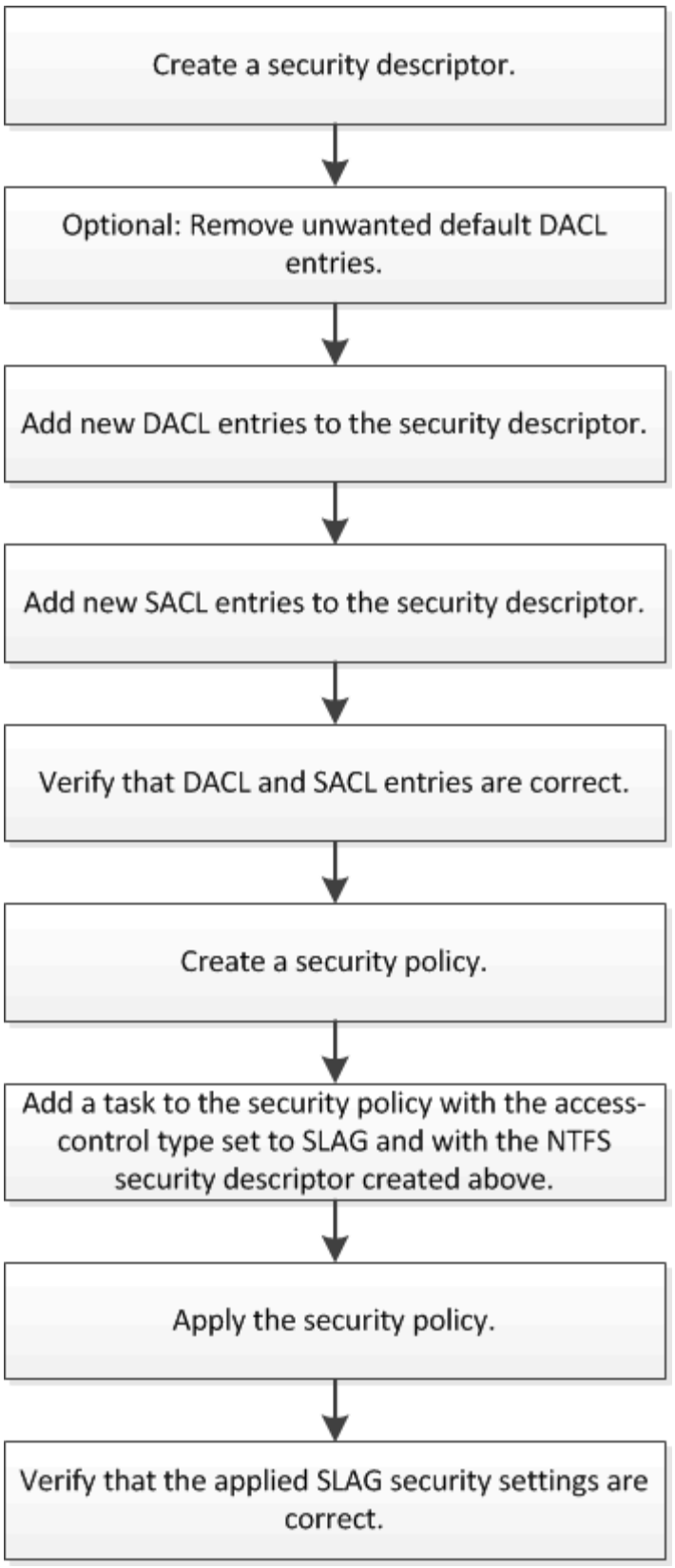
- Proteção da propriedade intelectual através da auditoria e controlo do acesso de todos os utilizadores ao

nível do armazenamento

- Armazenamento para empresas de serviços financeiros, incluindo bancos e grupos de negociação
- Serviços governamentais dos EUA com storage de arquivos separado para departamentos individuais
- Universidades protegendo todos os arquivos dos alunos

Fluxo de trabalho para configurar o Storage-Level Access Guard

O fluxo de trabalho para configurar o guarda de acesso em nível de armazenamento (SLAG) usa os mesmos comandos CLI do ONTAP que você usa para configurar permissões de arquivos NTFS e políticas de auditoria. Em vez de configurar o acesso a arquivos e diretórios em um destino designado, você configura O SLAG no volume designado de máquina virtual de armazenamento (SVM).



Informações relacionadas

Configurando o Storage-Level Access Guard

Configurar o Storage-Level Access Guard

Há uma série de etapas que você precisa seguir para configurar o Storage-Level Access Guard em um volume ou qtree. O Storage-Level Access Guard fornece um nível de segurança de acesso definido no nível de armazenamento. Ele fornece segurança que se aplica a todos os acessos de todos os protocolos nas ao objeto de storage ao qual foi aplicado.

Passos

1. Crie um descritor de segurança usando o `vserver security file-directory ntfs create` comando.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Um descritor de segurança é criado com as quatro entradas de controle de acesso (ACEs) padrão a seguir:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Se você não quiser usar as entradas padrão ao configurar o Storage-Level Access Guard, você pode removê-las antes de criar e adicionar seus próprios ACEs ao descritor de segurança.

2. Remova qualquer um dos ACEs DACL padrão do descritor de segurança que você não deseja configurar

com segurança Storage-Level Access Guard:

a. Remova quaisquer ACEs DACL indesejados usando o `vserver security file-directory ntfs dacl remove` comando.

   Neste exemplo, três ACEs DACL padrão são removidos do descritor de segurança: BUILTIN/Administrators, BUILTIN/Users e CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Verifique se os ACEs DACL que você não deseja usar para a segurança Storage-Level Access Guard são removidos do descritor de segurança usando o `vserver security file-directory ntfs dacl show` comando.

   Neste exemplo, a saída do comando verifica se três ACEs DACL padrão foram removidos do descritor de segurança, deixando apenas a entrada DACA ACE padrão DA AUTORIDADE NT/SISTEMA:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Adicione uma ou mais entradas DACL a um descritor de segurança usando o `vserver security file-directory ntfs dacl add` comando.

   Neste exemplo, dois ACEs DACL são adicionados ao descritor de segurança:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Adicione uma ou mais entradas SACL a um descritor de segurança usando o `vserver security file-directory ntfs sacl add` comando.

   Neste exemplo, dois ACEs SACL são adicionados ao descritor de segurança:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verifique se os ACEs DACL e SACL estão configurados corretamente utilizando os `vserver security file-directory ntfs dacl show` comandos e `vserver security file-directory ntfs sacl show`, respetivamente.

   Neste exemplo, o comando a seguir exibe informações sobre entradas DACL para descritor de segurança "D1":

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Neste exemplo, o comando a seguir exibe informações sobre entradas SACL para descritor de segurança "D1":

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Crie uma política de segurança usando o `vserver security file-directory policy create` comando.

   O exemplo a seguir cria uma política chamada "policy1":

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Verifique se a política está corretamente configurada usando o `vserver security file-directory policy show` comando.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança usando o `vserver security file-directory policy task add` comando com o `-access-control` parâmetro definido como `slag`.

   Mesmo que uma política possa conter mais de uma tarefa Storage-Level Access Guard, você não pode configurar uma política para conter tarefas de diretório de arquivo e Guarda de acesso no nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

   Neste exemplo, uma tarefa é adicionada à política chamada "'policy1", que é atribuída ao descritor de segurança "'D1'". Ele é atribuído ao `/datavol1` caminho com o tipo de controle de acesso definido como "lag".

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Verifique se a tarefa está configurada corretamente usando o `vserver security file-directory`

`policy task show` comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Aplique a política de segurança Storage-Level Access Guard usando o `vserver security file-directory apply` comando.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    O trabalho para aplicar a política de segurança está agendado.

11. Verifique se as configurações de segurança do Access Guard no nível de armazenamento aplicado estão corretas usando o `vserver security file-directory show` comando.

    Neste exemplo, a saída do comando mostra que a segurança do Storage-Level Access Guard foi aplicada ao volume NTFS `/datavol1` . Mesmo que a DACL padrão que permite o controle total para todos permaneça, a segurança do Storage-Level Access Guard restringe (e audita) o acesso aos grupos definidos nas configurações do Storage-Level Access Guard.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informações relacionadas

Gerenciamento da segurança de arquivos NTFS, políticas de auditoria NTFS e Guarda de acesso em nível de armazenamento em SVMs usando a CLI

Fluxo de trabalho para configurar o Storage-Level Access Guard

Exibindo informações sobre o Storage-Level Access Guard

Remoção do Storage-Level Access Guard

Matriz DE ESCÓRIA eficaz

Você pode configurar O SLAG em um volume ou uma qtree ou ambos. A matriz DE ESCÓRIA define em que volume ou qtree é a configuração DE ESCÓRIA aplicável em vários cenários listados na tabela.

	ESCÓRIA de volume num AFS	**ESCÓRIA de volume em uma cópia Snapshot**	**ESCÓRIA de Qtree em um AFS**	**ESCÓRIA de Qtree em uma cópia Snapshot**
Acesso de volume num sistema de ficheiros de acesso (AFS)	SIM	NÃO	N/A.	N/A.
Acesso de volume em uma cópia Snapshot	SIM	NÃO	N/A.	N/A.
Acesso Qtree em um AFS (quando ESCÓRIA está presente na qtree)	NÃO	NÃO	SIM	NÃO
Acesso Qtree em um AFS (quando ESCÓRIA não está presente em qtree)	SIM	NÃO	NÃO	NÃO
Acesso Qtree na cópia Snapshot (quando A ESCÓRIA está presente no qtree AFS)	NÃO	NÃO	SIM	NÃO
Acesso Qtree na cópia Snapshot (quando A ESCÓRIA não está presente na qtree AFS)	SIM	NÃO	NÃO	NÃO

Exibir informações sobre o Storage-Level Access Guard

O Storage-Level Access Guard é uma terceira camada de segurança aplicada em um volume ou qtree. As configurações do Access Guard no nível de armazenamento não podem ser visualizadas usando a janela Propriedades do Windows. Você deve usar a CLI do ONTAP para exibir informações sobre a segurança do Guarda de acesso em nível de armazenamento, que pode ser usada para validar sua configuração ou para

solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para o volume ou qtree cujas informações de segurança do Storage-Level Access Guard você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

Passo

1. Exibir as configurações de segurança do Access Guard no nível de armazenamento com o nível de detalhe desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Com detalhes expandidos	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemplos

O exemplo a seguir exibe informações de segurança do Access Guard no nível de armazenamento para o volume de estilo de segurança NTFS com o caminho `/datavol1` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

O exemplo a seguir exibe as informações do Access Guard no nível de storage sobre o volume de estilo de segurança misto no caminho `/datavol5` do SVM VS1. O nível superior deste volume tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Remova o Storage-Level Access Guard

Você pode remover o Storage-Level Access Guard em um volume ou qtree se não quiser mais definir a segurança de acesso no nível de armazenamento. A remoção do Storage-Level Access Guard não modifica ou remove a segurança regular do arquivo NTFS e do diretório.

Passos

1. Verifique se o volume ou a qtree tem o Storage-Level Access Guard configurado usando o `vserver security file-directory show` comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Remova o Storage-Level Access Guard usando o `vserver security file-directory remove-slag` comando.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Verifique se o Storage-Level Access Guard foi removido do volume ou qtree usando o `vserver security file-directory show` comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gerencie o acesso a arquivos usando SMB

Use usuários e grupos locais para autenticação e autorização

Como o ONTAP usa usuários e grupos locais

Conceitos de usuários e grupos locais

Você deve saber o que são usuários e grupos locais e algumas informações básicas sobre eles, antes de determinar se deseja configurar e usar usuários e grupos locais em seu ambiente.

- **Usuário local**

  Uma conta de usuário com um identificador de segurança exclusivo (SID) que tem visibilidade somente na máquina virtual de armazenamento (SVM) na qual é criada. As contas de usuário locais têm um conjunto de atributos, incluindo nome de usuário e SID. Uma conta de usuário local autentica localmente no servidor CIFS usando autenticação NTLM.

  As contas de usuário têm vários usos:

  - Usado para conceder *Gerenciamento de Direitos de Usuário* Privileges a um usuário.
  - Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.

- **Grupo local**

  Um grupo com um SID exclusivo tem visibilidade somente na SVM em que ele é criado. Grupos contêm um conjunto de membros. Os membros podem ser usuários locais, usuários de domínio, grupos de domínio e contas de máquinas de domínio. Os grupos podem ser criados, modificados ou excluídos.

  Os grupos têm vários usos:

  - Usado para conceder *Gerenciamento de Direitos de Usuário* Privileges aos seus membros.
  - Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.
- **Domínio local**

  Um domínio que tem escopo local, limitado pelo SVM. O nome do domínio local é o nome do servidor CIFS. Os usuários e grupos locais estão contidos no domínio local.

- **Identificador de segurança (SID)**

  Um SID é um valor numérico de comprimento variável que identifica os princípios de segurança do estilo Windows. Por exemplo, um SID típico assume a seguinte forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- * Autenticação NTLM*

  Um método de segurança do Microsoft Windows usado para autenticar usuários em um servidor CIFS.

- **Banco de dados replicado em cluster (RDB)**

  Um banco de dados replicado com uma instância em cada nó em um cluster. Os objetos de usuário local e grupo são armazenados no RDB.

Razões para criar usuários locais e grupos locais

Há várias razões para criar usuários locais e grupos locais na sua máquina virtual de storage (SVM). Por exemplo, você pode acessar um servidor SMB usando uma conta de usuário local se os controladores de domínio (DCs) não estiverem disponíveis, talvez queira usar grupos locais para atribuir Privileges ou se o servidor SMB estiver em um grupo de trabalho.

Você pode criar uma ou mais contas de usuário locais pelos seguintes motivos:

- Seu servidor SMB está em um grupo de trabalho e os usuários de domínio não estão disponíveis.

  Os utilizadores locais são necessários nas configurações do grupo de trabalho.

- Você deseja a capacidade de autenticar e fazer login no servidor SMB se os controladores de domínio não estiverem disponíveis.

  Os usuários locais podem se autenticar com o servidor SMB usando a autenticação NTLM quando o controlador de domínio está inativo ou quando problemas de rede impedem que o servidor SMB entre em Contato com o controlador de domínio.

- Você deseja atribuir *User Rights Management* Privileges a um usuário local.

User Rights Management é a capacidade de um administrador de servidor SMB controlar quais direitos os usuários e grupos têm no SVM. Você pode atribuir Privileges a um usuário atribuindo o Privileges à conta do usuário ou tornando o usuário membro de um grupo local que tenha esses Privileges.

Você pode criar um ou mais grupos locais pelos seguintes motivos:

- O servidor SMB está em um grupo de trabalho e os grupos de domínio não estão disponíveis.

  Os grupos locais não são necessários nas configurações do grupo de trabalho, mas podem ser úteis para gerenciar o Access Privileges para usuários locais do grupo de trabalho.

- Você deseja controlar o acesso aos recursos de arquivos e pastas usando grupos locais para controle de compartilhamento e acesso a arquivos.
- Você deseja criar grupos locais com *User Rights Management* Privileges personalizado.

  Alguns grupos de utilizadores incorporados têm Privileges predefinidos. Para atribuir um conjunto personalizado de Privileges, você pode criar um grupo local e atribuir o Privileges necessário a esse grupo. Em seguida, você pode adicionar usuários locais, usuários de domínio e grupos de domínio ao grupo local.

Informações relacionadas

Como funciona a autenticação de usuário local

Lista de Privileges suportados

Como funciona a autenticação de usuário local

Antes que um usuário local possa acessar dados em um servidor CIFS, o usuário deve criar uma sessão autenticada.

Como o SMB é baseado em sessão, a identidade do usuário pode ser determinada apenas uma vez, quando a sessão é configurada pela primeira vez. O servidor CIFS usa autenticação baseada em NTLM ao autenticar usuários locais. Tanto o NTLMv1 como o NTLMv2 são suportados.

O ONTAP usa autenticação local em três casos de uso. Cada caso de uso depende se a parte do domínio do nome de usuário (com o formato DOMÍNIO/usuário) corresponde ao nome de domínio local do servidor CIFS (o nome do servidor CIFS):

- A parte do domínio corresponde

  Os usuários que fornecem credenciais de usuário local ao solicitar acesso aos dados são autenticados localmente no servidor CIFS.

- A parte do domínio não corresponde

  O ONTAP tenta usar a autenticação NTLM com um controlador de domínio no domínio ao qual o servidor CIFS pertence. Se a autenticação for bem-sucedida, o login será concluído. Se não for bem-sucedido, o que acontece a seguir depende do motivo pelo qual a autenticação não foi bem-sucedida.

  Por exemplo, se o usuário existir no ative Directory mas a senha for inválida ou expirada, o ONTAP não tentará usar a conta de usuário local correspondente no servidor CIFS. Em vez disso, a autenticação falha. Existem outros casos em que o ONTAP usa a conta local correspondente no servidor CIFS, se existir, para autenticação - mesmo que os nomes de domínio NetBIOS não correspondam. Por exemplo,

se existir uma conta de domínio correspondente mas estiver desativada, o ONTAP utiliza a conta local correspondente no servidor CIFS para autenticação.

- A parte do domínio não é especificada

  O ONTAP tenta pela primeira vez a autenticação como um usuário local. Se a autenticação como um usuário local falhar, o ONTAP autenticará o usuário com um controlador de domínio no domínio ao qual o servidor CIFS pertence.

Depois que a autenticação de usuário local ou de domínio for concluída com sucesso, o ONTAP constrói um token de acesso completo de usuário, que leva em conta a associação de grupo local e o Privileges.

Para obter mais informações sobre autenticação NTLM para usuários locais, consulte a documentação do Microsoft Windows.

Informações relacionadas

Ativar ou desativar a autenticação de utilizador local

Como os tokens de acesso do usuário são construídos

Quando um usuário mapeia um compartilhamento, uma sessão SMB autenticada é estabelecida e um token de acesso de usuário é construído que contém informações sobre o usuário, a associação de grupo do usuário e Privileges cumulativos e o usuário UNIX mapeado.

A menos que a funcionalidade esteja desativada, as informações de usuário local e grupo também são adicionadas ao token de acesso do usuário. A forma como os tokens de acesso são construídos depende se o login é para um usuário local ou um usuário de domínio do ative Directory:

- Início de sessão do utilizador local

  Embora os usuários locais possam ser membros de diferentes grupos locais, os grupos locais não podem ser membros de outros grupos locais. O token de acesso de usuário local é composto por uma união de todos os Privileges atribuídos a grupos aos quais um usuário local específico é membro.

- Login de usuário de domínio

  Quando um usuário de domínio faz login, o ONTAP obtém um token de acesso de usuário que contém o SID do usuário e os SIDs para todos os grupos de domínio aos quais o usuário é membro. O ONTAP usa a união do token de acesso do usuário de domínio com o token de acesso fornecido por associações locais dos grupos de domínio do usuário (se houver), bem como qualquer Privileges direto atribuído ao usuário do domínio ou qualquer uma de suas associações de grupo de domínio.

Para login de usuário local e de domínio, o RID de grupo principal também é definido para o token de acesso do usuário. O RID predefinido é `Domain Users` (RID 513). Não é possível alterar a predefinição.

O processo de mapeamento de nomes do Windows para UNIX e UNIX para Windows segue as mesmas regras para contas locais e de domínio.

> Não há mapeamento automático implícito de um usuário UNIX para uma conta local. Se isso for necessário, uma regra de mapeamento explícito deve ser especificada usando os comandos de mapeamento de nomes existentes.

Diretrizes para o uso do SnapMirror em SVMs que contêm grupos locais

Você deve estar ciente das diretrizes ao configurar o SnapMirror em volumes de propriedade de SVMs que contêm grupos locais.

Não é possível usar grupos locais em ACEs aplicados a arquivos, diretórios ou compartilhamentos replicados pelo SnapMirror para outro SVM. Se você usar o recurso SnapMirror para criar um espelhamento de DR para um volume em outro SVM e o volume tiver um ACE para um grupo local, o ACE não será válido no espelhamento. Se os dados forem replicados para uma SVM diferente, eles serão migrados para um domínio local diferente. As permissões concedidas a usuários e grupos locais são válidas somente dentro do escopo do SVM no qual foram criados originalmente.

O que acontece com usuários e grupos locais ao excluir servidores CIFS

O conjunto padrão de usuários e grupos locais é criado quando um servidor CIFS é criado e eles são associados à máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS. Os administradores do SVM podem criar usuários e grupos locais a qualquer momento. Você precisa estar ciente do que acontece com usuários e grupos locais quando você exclui o servidor CIFS.

Usuários e grupos locais estão associados a SVMs; portanto, eles não são excluídos quando os servidores CIFS são excluídos devido a considerações de segurança. Embora os usuários e grupos locais não sejam excluídos quando o servidor CIFS é excluído, eles ficam ocultos. Não é possível exibir ou gerenciar usuários e grupos locais até que você crie novamente um servidor CIFS no SVM.

O status administrativo do servidor CIFS não afeta a visibilidade de usuários ou grupos locais.

Como você pode usar o Microsoft Management Console com usuários e grupos locais

Você pode exibir informações sobre usuários e grupos locais no Console de Gerenciamento da Microsoft. Com esta versão do ONTAP, não é possível executar outras tarefas de gerenciamento para usuários e grupos locais a partir do Console de Gerenciamento da Microsoft.

Diretrizes para reverter

Se você pretende reverter o cluster para uma versão do ONTAP que não ofereça suporte a usuários e grupos locais e usuários e grupos locais estejam sendo usados para gerenciar o acesso a arquivos ou direitos de usuário, você deve estar ciente de certas considerações.

- Devido a razões de segurança, as informações sobre usuários locais configurados, grupos e Privileges não são excluídas quando o ONTAP é revertido para uma versão que não suporta a funcionalidade de usuários locais e grupos.
- Após a reversão para uma versão principal anterior do ONTAP, o ONTAP não usa usuários e grupos locais durante a autenticação e criação de credenciais.
- Os utilizadores e grupos locais não são removidos das ACLs de ficheiros e pastas.
- Solicitações de acesso a arquivos que dependem do acesso concedido devido às permissões concedidas a usuários ou grupos locais são negadas.

Para permitir o acesso, você deve reconfigurar as permissões de arquivo para permitir o acesso com base em objetos de domínio em vez de objetos de usuário local e grupo.

O que são os Privileges locais

Lista de Privileges suportados

O ONTAP tem um conjunto predefinido de Privileges suportados. Alguns grupos locais predefinidos têm alguns desses Privileges adicionados a eles por padrão. Você também pode adicionar ou remover Privileges dos grupos predefinidos ou criar novos usuários ou grupos locais e adicionar Privileges aos grupos criados ou aos usuários e grupos de domínio existentes.

A tabela a seguir lista os Privileges suportados na máquina virtual de armazenamento (SVM) e fornece uma lista de grupos BUILTIN com Privileges atribuídos:

Nome do privilégio	Configuração de segurança padrão	Descrição
`SeTcbPrivilege`	Nenhum	Agir como parte do sistema operacional
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Faça backup de arquivos e diretórios, substituindo quaisquer ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaure arquivos e diretórios, substituindo qualquer ACLs defina qualquer SID válido de usuário ou grupo como proprietário do arquivo
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Assuma a propriedade de arquivos ou outros objetos
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gerenciar a auditoria Isso inclui a visualização, o dumping e a limpeza do log de segurança.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators` `BUILTIN\Backup Operators`,, `BUILTIN\Power Users` `BUILTIN\Users`,,, `Everyone`	Verificação da travessa de derivação Os usuários com esse privilégio não são obrigados a ter permissões de avanço (x) para percorrer pastas, links simbólicos ou junções.

Informações relacionadas

- Atribuir Privileges local
- Configuração da verificação transversal de derivação

Atribuir Privileges

Você pode atribuir Privileges diretamente a usuários locais ou usuários de domínio. Como alternativa, você pode atribuir usuários a grupos locais cujos Privileges atribuídos correspondem aos recursos que você deseja que esses usuários tenham.

- Você pode atribuir um conjunto de Privileges a um grupo que você criar.

  Em seguida, adicione um utilizador ao grupo que tem o Privileges que pretende que esse utilizador tenha.

- Você também pode atribuir usuários locais e usuários de domínio a grupos predefinidos cujo Privileges padrão corresponde ao Privileges que você deseja conceder a esses usuários.

Informações relacionadas

- Adicionando Privileges a usuários ou grupos locais ou de domínio
- Removendo Privileges de usuários ou grupos locais ou de domínio
- Redefinir o Privileges para usuários e grupos locais ou de domínio
- Configuração da verificação transversal de derivação

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Há certas diretrizes que você deve ter em mente quando você usa grupos BUILTIN e a conta de administrador local. Por exemplo, você pode renomear a conta de administrador local, mas não pode excluir essa conta.

- A conta de administrador pode ser renomeada, mas não pode ser excluída.
- A conta de administrador não pode ser removida do grupo BUILTIN/Administradores.
- Os grupos DE COMPILAÇÃO podem ser renomeados, mas não podem ser excluídos.

  Depois que o grupo BUILTIN é renomeado, outro objeto local pode ser criado com o nome conhecido; no entanto, o objeto recebe um novo RID.

- Não existe uma conta de convidado local.

Informações relacionadas

Grupos BUILTIN predefinidos e Privileges padrão

Requisitos para senhas de usuários locais

Por padrão, as senhas de usuário local devem atender aos requisitos de complexidade. Os requisitos de complexidade de senha são semelhantes aos requisitos definidos na política de segurança local do Microsoft Windows *diretiva de segurança*.

A senha deve atender aos seguintes critérios:

- Deve ter pelo menos seis carateres de comprimento

- Não deve conter o nome da conta de utilizador
- Deve conter carateres de pelo menos três das quatro categorias seguintes:
  - Carateres maiúsculos em inglês (A a Z)
  - Carateres minúsculos em inglês (a a z)
  - Base 10 dígitos (0 a 9)
  - Carateres especiais:
    i. ! ( ) [ ] : ; " ' > , . ? /

Informações relacionadas

Ativar ou desativar a complexidade de senha necessária para usuários SMB locais

Exibindo informações sobre as configurações de segurança do servidor CIFS

Alterando senhas de contas de usuário locais

Grupos BUILTIN predefinidos e Privileges padrão

Você pode atribuir a associação de um usuário local ou usuário de domínio a um conjunto predefinido de grupos BUILTIN fornecidos pelo ONTAP. Grupos predefinidos têm Privileges predefinidos atribuídos.

A tabela a seguir descreve os grupos predefinidos:

Grupo BUILTIN predefinido	Privileges padrão
`BUILTIN\Administrators`LIVRAR-SE 544 Quando criada pela primeira vez, a conta local `Administrator`, com um RID de 500, é automaticamente feita um membro deste grupo. Quando a máquina virtual de storage (SVM) é unida a um domínio, o `domain\Domain Admins` grupo é adicionado ao grupo. Se o SVM sair do domínio, o `domain\Domain Admins` grupo será removido do grupo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`LIVRAR-SE 547 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo têm as seguintes caraterísticas: • Pode criar e gerenciar usuários e grupos locais. • Não é possível adicionar a si mesmos ou qualquer outro objeto ao `BUILTIN\Administrators` grupo.	`SeChangeNotifyPrivilege`

Grupo BUILTIN predefinido	Privileges padrão
`BUILTIN\Backup Operators`LIVRAR-SE 551 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo podem substituir as permissões de leitura e gravação em arquivos ou pastas se forem abertos com intenção de backup.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`LIVRAR-SE 545 Quando criado pela primeira vez, este grupo não tem nenhum membro (além do grupo especial implícito `Authenticated Users`). Quando o SVM é associado a um domínio, o `domain\Domain Users` grupo é adicionado a esse grupo. Se o SVM sair do domínio, o `domain\Domain Users` grupo será removido desse grupo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Este grupo inclui todos os utilizadores, incluindo convidados (mas não utilizadores anónimos). Este é um grupo implícito com uma associação implícita.	`SeChangeNotifyPrivilege`

Informações relacionadas

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Lista de Privileges suportados

Configuração da verificação transversal de derivação

Ativar ou desativar a funcionalidade de utilizadores e grupos locais

Ative ou desative a visão geral da funcionalidade de usuários e grupos locais

Antes de poder utilizar utilizadores e grupos locais para o controlo de acesso de dados de estilo de segurança NTFS, a funcionalidade de grupo e utilizador local tem de estar ativada. Além disso, se você quiser usar usuários locais para autenticação SMB, a funcionalidade de autenticação de usuário local deve estar ativada.

A funcionalidade de utilizadores e grupos locais e a autenticação de utilizadores locais são ativadas por predefinição. Se eles não estiverem ativados, você deverá ativá-los antes de configurar e usar usuários e grupos locais. Você pode desativar a funcionalidade de usuários e grupos locais a qualquer momento.

Além de desabilitar explicitamente a funcionalidade de usuário local e grupo, o ONTAP desabilita a funcionalidade de usuário local e grupo se qualquer nó no cluster for revertido para uma versão do ONTAP que não ofereça suporte à funcionalidade. A funcionalidade de usuário e grupo local não é ativada até que todos os nós do cluster estejam executando uma versão do ONTAP que o suporte.

Informações relacionadas

Modificar contas de usuário locais

Modificar grupos locais

Adicione Privileges a usuários ou grupos locais ou de domínio

Ative ou desative usuários e grupos locais

Você pode ativar ou desativar usuários locais e grupos para acesso SMB em máquinas virtuais de armazenamento (SVMs). A funcionalidade de utilizadores e grupos locais está ativada por predefinição.

Sobre esta tarefa

Você pode usar usuários e grupos locais ao configurar permissões de compartilhamento SMB e arquivos NTFS e pode, opcionalmente, usar usuários locais para autenticação ao criar uma conexão SMB. Para utilizar utilizadores locais para autenticação, também tem de ativar a opção de autenticação utilizadores locais e grupos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que os usuários e grupos locais sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a funcionalidade de usuários e grupos locais no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Ativar ou desativar a autenticação de utilizador local

Ativar ou desativar contas de utilizador locais

Ativar ou desativar a autenticação de utilizador local

Você pode ativar ou desativar a autenticação de usuário local para acesso SMB em máquinas virtuais de armazenamento (SVMs). O padrão é permitir a autenticação de usuário local, o que é útil quando o SVM não pode entrar em Contato com um controlador de domínio ou se você optar por não usar controles de acesso em nível de domínio.

Antes de começar

A funcionalidade de usuários e grupos locais deve estar ativada no servidor CIFS.

Sobre esta tarefa

Você pode ativar ou desativar a autenticação de usuário local a qualquer momento. Se você quiser usar usuários locais para autenticação ao criar uma conexão SMB, também deverá ativar a opção usuários e grupos locais do servidor CIFS.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que a autenticação local seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a autenticação de usuário local no SVM VS1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Como funciona a autenticação de usuário local

Ativar ou desativar utilizadores e grupos locais

Gerenciar contas de usuários locais

Modificar contas de usuário locais

Você pode modificar uma conta de usuário local se quiser alterar o nome completo ou a descrição de um usuário existente e se quiser ativar ou desativar a conta de usuário. Você também pode renomear uma conta de usuário local se o nome do usuário estiver comprometido ou se uma alteração de nome for necessária para fins administrativos.

Se você quiser…	Digite o comando…
Modifique o nome completo do usuário local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Se o nome completo contiver um espaço, ele deve ser incluído entre aspas duplas.
Modifique a descrição do usuário local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Ative ou desative a conta de utilizador local	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is -account-disabled {true`
false}`	Renomeie a conta de usuário local

Exemplo

O exemplo a seguir renomeia o usuário local "'CIFS_SERVER'" para "'CIFS_Server' sue_new'" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Ativar ou desativar contas de utilizador locais

Você ativa uma conta de usuário local se quiser que o usuário possa acessar os dados contidos na máquina virtual de armazenamento (SVM) em uma conexão SMB. Você também pode desativar uma conta de usuário local se não quiser que esse usuário acesse dados do SVM em SMB.

Sobre esta tarefa

Você ativa um usuário local modificando a conta de usuário.

Passo

1. Execute a ação apropriada:

Se você quiser…	Digite o comando…
Ative a conta de utilizador	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is-account -disabled false`
Desative a conta de usuário	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is-account -disabled true`

Altere as senhas da conta de usuário local

Pode alterar a palavra-passe da conta de um utilizador local. Isso pode ser útil se a senha do usuário for comprometida ou se o usuário tiver esquecido a senha.

Passo

1. Altere a senha executando a ação apropriada: `vserver cifs users-and-groups local-user set-password -vserver` *vserver_name* `-user-name` *user_name*

Exemplo

O exemplo a seguir define a senha do usuário local "'CIFS_Server'" associada à máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Informações relacionadas

Ativar ou desativar a complexidade de senha necessária para usuários SMB locais

Exibindo informações sobre as configurações de segurança do servidor CIFS

Exibir informações sobre usuários locais

Você pode exibir uma lista de todos os usuários locais em um formulário de resumo. Se você quiser determinar quais configurações de conta estão configuradas para um usuário específico, você pode exibir informações detalhadas de conta para esse usuário, bem como as informações de conta para vários usuários. Essas informações podem ajudá-lo a determinar se você precisa modificar as configurações de um usuário e também solucionar problemas de autenticação ou acesso a arquivos.

Sobre esta tarefa

As informações sobre a palavra-passe de um utilizador nunca são apresentadas.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Exibir informações sobre todos os usuários na máquina virtual de storage (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Exibir informações detalhadas da conta para um usuário	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

Há outros parâmetros opcionais que você pode escolher quando você executa o comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os usuários locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Exibir informações sobre associações de grupos para usuários locais

Você pode exibir informações sobre os grupos locais aos quais um usuário local pertence. Você pode usar essas informações para determinar qual acesso o usuário deve ter aos arquivos e pastas. Essas informações podem ser úteis para determinar quais direitos de acesso o usuário deve ter a arquivos e pastas ou ao solucionar problemas de acesso ao arquivo.

Sobre esta tarefa

Você pode personalizar o comando para exibir apenas as informações que deseja ver.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Exibir informações de associação de usuário local para um usuário local especificado	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Exibir informações de associação de usuários locais para o grupo local do qual esse usuário local é membro	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Exibir informações de associação de usuários para usuários locais associados a uma máquina virtual de armazenamento (SVM) especificada	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Exibir informações detalhadas de todos os usuários locais em um SVM especificado	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe as informações de associação para todos os usuários locais no SVM VS1; o usuário "CIFS_SERVER" é membro do grupo "BUILTIN" Administradores, e "'CIFS_Server'" é membro do grupo "'CIFS_Server' G1":

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                    Membership
---------- ---------------------------- ----------------------
vs1        CIFS_SERVER\Administrator    BUILTIN\Administrators
           CIFS_SERVER\sue              CIFS_SERVER\g1
```

Eliminar contas de utilizador locais

Você pode excluir contas de usuários locais da máquina virtual de storage (SVM) se elas não forem mais necessárias para a autenticação SMB local para o servidor CIFS ou para determinar os direitos de acesso aos dados contidos no SVM.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir usuários locais:

- O sistema de ficheiros não foi alterado.

  Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse usuário não são ajustados.

- Todas as referências a usuários locais são removidas dos bancos de dados de associação e Privileges.
- Usuários padrão e bem conhecidos, como Administrador, não podem ser excluídos.

Passos

1. Determine o nome da conta de usuário local que você deseja excluir: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Eliminar o utilizador local: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Verifique se a conta de usuário foi excluída: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exclui o usuário local "'CIFS_Server'" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Gerenciar grupos locais

Modificar grupos locais

Você pode modificar grupos locais existentes alterando a descrição de um grupo local existente ou renomeando o grupo.

Se você quiser…	Use o comando…
Modifique a descrição do grupo local	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Renomeie o grupo local	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Exemplos

O exemplo a seguir renomeia o grupo local "'CIFS_SERVER' Engineering" para "'CIFS_Server' Engineering_new'":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

O exemplo a seguir modifica a descrição do grupo local "'CIFS_SERVER' Engineering":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Exibir informações sobre grupos locais

É possível exibir uma lista de todos os grupos locais configurados no cluster ou em uma máquina virtual de armazenamento (SVM) especificada. Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos para dados contidos no SVM ou problemas de direitos de usuário (privilégios) no SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser informações sobre…	Digite o comando…
Todos os grupos locais no cluster	`vserver cifs users-and-groups local-group show`
Todos os grupos locais no SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

   Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Diretrizes para adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- O grupo local deve existir antes de poder adicionar um utilizador a ele.
- O utilizador tem de existir antes de poder adicionar o utilizador a um grupo local.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o Data ONTAP deve ser capaz de resolver o nome para um SID.

Diretrizes para remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- O grupo do qual você deseja remover um membro deve existir.
- O ONTAP deve ser capaz de resolver os nomes dos membros que você deseja remover do grupo para um SID correspondente.

Passo

1. Adicione ou remova um membro em um grupo.

Se você quiser…	Em seguida, use o comando…
Adicione um membro a um grupo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.
Remova um membro de um grupo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.

O exemplo a seguir adiciona um usuário local "'SMB_SERVER'" e um grupo de domínio "'AD_Dom_eng'" ao grupo local "'SMB_SERVER' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

O exemplo a seguir remove os usuários locais "'SMB_SERVER'" e "'SMB_SERVER' james' do grupo local

"'SMB_Server' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informações relacionadas

Exibindo informações sobre membros de grupos locais

Exibir informações sobre membros de grupos locais

É possível exibir uma lista de todos os membros de grupos locais configurados no cluster ou em uma máquina virtual de armazenamento especificada (SVM). Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos ou problemas de direitos de usuário (privilégios).

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Membros de todos os grupos locais no cluster	`vserver cifs users-and-groups local-group show-members`
Membros de todos os grupos locais no SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe informações sobre membros de todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Eliminar um grupo local

Você poderá excluir um grupo local da máquina virtual de storage (SVM) se não for mais necessário para determinar direitos de acesso a dados associados a esse SVM ou se não for mais necessário atribuir direitos de usuário (Privileges) a membros do grupo.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir grupos locais:

- O sistema de ficheiros não foi alterado.

  Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse grupo não são ajustados.

- Se o grupo não existir, um erro será retornado.
- O grupo especial *todos* não pode ser excluído.
- Grupos internos, como *BUILTIN__BUILTIN/Users*, não podem ser excluídos.

Passos

1. Determine o nome do grupo local que você deseja excluir exibindo a lista de grupos locais no SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Eliminar o grupo local: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Verifique se o grupo foi excluído: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exclui o grupo local "CIFS_SERVER" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Atualizar nomes de usuários e grupos de domínio em bancos de dados locais

Você pode adicionar usuários e grupos de domínio aos grupos locais de um servidor CIFS. Esses objetos de domínio são registrados em bancos de dados locais no cluster. Se um objeto de domínio for renomeado, os bancos de dados locais devem ser atualizados manualmente.

Sobre esta tarefa

Você deve especificar o nome da máquina virtual de armazenamento (SVM) na qual deseja atualizar nomes de domínio.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute a ação apropriada:

Se você quiser atualizar usuários e grupos de domínio e…	Use este comando…
Exibir usuários e grupos de domínio que foram atualizados com êxito e que falharam na atualização	`vserver cifs users-and-groups update-names -vserver` *vserver_name*

Se você quiser atualizar usuários e grupos de domínio e…	Use este comando…
Exibir usuários e grupos de domínio que foram atualizados com êxito	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Exiba apenas os usuários e grupos de domínio que não conseguem atualizar	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Suprimir todas as informações de status sobre atualizações	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir atualiza os nomes de usuários e grupos de domínio associados à máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Para a última atualização, há uma cadeia de nomes dependente que precisa ser atualizada:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gerenciar Privileges local

Adicione Privileges a usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio adicionando o Privileges. O Privileges adicionado substitui o Privileges padrão atribuído a qualquer um desses objetos. Isso fornece segurança aprimorada, permitindo que você personalize o que o Privileges um usuário ou grupo tem.

Antes de começar

O usuário ou grupo local ou domínio ao qual o Privileges será adicionado já deve existir.

Sobre esta tarefa

Adicionar um privilégio a um objeto substitui o Privileges padrão para esse usuário ou grupo. Adicionar um privilégio não remove Privileges adicionados anteriormente.

Você deve ter em mente o seguinte ao adicionar o Privileges a usuários ou grupos locais ou de domínio:

- Você pode adicionar um ou mais Privileges.
- Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio.

  O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Adicione um ou mais Privileges a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados são aplicados ao objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O exemplo a seguir adiciona o "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do Privileges ao usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

Remova o Privileges de usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio removendo o Privileges. Isso fornece segurança aprimorada, permitindo que você

personalize o Privileges máximo que os usuários e grupos têm.

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Você deve ter em mente o seguinte ao remover o Privileges de usuários ou grupos locais ou de domínio:

- Você pode remover um ou mais Privileges.
- Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio.

  O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Remova um ou mais Privileges de um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group -name _name_ -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados foram removidos do objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O exemplo a seguir remove o Privileges "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Redefinir o Privileges para usuários e grupos locais ou de domínio

Você pode redefinir o Privileges para usuários e grupos locais ou de domínio. Isso pode ser útil quando você fez modificações no Privileges para um usuário ou grupo local ou de domínio e essas modificações não são mais desejadas ou necessárias.

Sobre esta tarefa

A redefinição do Privileges para um usuário ou grupo local ou de domínio remove quaisquer entradas de privilégio para esse objeto.

Passos

1. Redefina o Privileges em um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verifique se os Privileges são redefinidos no objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplos

O exemplo a seguir redefine o Privileges no usuário "CIFS_SERVER" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1. Por padrão, os usuários normais não têm o Privileges associado às suas contas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

O exemplo a seguir redefine o Privileges para o grupo "Administradores", removendo efetivamente a entrada de privilégio:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Exibir informações sobre substituições de privilégios

Você pode exibir informações sobre Privileges personalizados atribuídos a grupos ou

contas de usuário locais ou de domínio. Essas informações ajudam a determinar se os direitos de usuário desejados são aplicados.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite este comando…
Privileges personalizado para todos os usuários e grupos de domínio e locais na máquina virtual de storage (SVM)	`vserver cifs users-and-groups privilege show -vserver vserver_name`
Privileges personalizado para um domínio específico ou usuário local e grupo no SVM	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O comando a seguir exibe todos os Privileges explicitamente associados a usuários e grupos locais ou de domínio para o SVM VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configure a verificação de desvio transversal

Configure a visão geral da verificação da travessia de derivação

A verificação de desvio transversal é um direito de usuário (também conhecido como *privilégio*) que determina se um usuário pode percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões no diretório atravessado. Você deve entender o que acontece ao permitir ou desativar a verificação de desvio transversal e como configurar a verificação de desvio transversal para usuários em máquinas virtuais de armazenamento (SVMs).

O que acontece ao permitir ou ao desativar a verificação transversal de desvio

- Se permitido, quando um usuário tenta acessar um arquivo, o ONTAP não verifica a permissão de avanço para os diretórios intermediários ao determinar se deve conceder ou negar acesso ao arquivo.
- Se não for permitido, o ONTAP verifica a permissão de avanço (execução) para todos os diretórios no

caminho para o arquivo.

Se qualquer um dos diretórios intermediários não tiver o "X" (permissão de avanço), o ONTAP nega o acesso ao arquivo.

Configure a verificação de desvio transversal

Você pode configurar a verificação de desvio transversal usando a CLI do ONTAP ou configurando políticas de grupo do ative Directory com esse direito de usuário.

O `SeChangeNotifyPrivilege` privilégio controla se os usuários têm permissão para ignorar a verificação transversal.

- Adicioná-lo a usuários ou grupos SMB locais na SVM ou a usuários ou grupos de domínio permite a verificação de desvio transversal.
- Removê-lo de usuários ou grupos SMB locais no SVM ou de usuários ou grupos de domínio não permite a verificação de desvio transversal.

Por padrão, os seguintes grupos BUILTIN no SVM têm o direito de ignorar a verificação transversal:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Se você não quiser permitir que membros de um desses grupos ignorem a verificação transversal, você deve remover esse privilégio do grupo.

Você deve ter em mente o seguinte ao configurar a verificação de desvio transversal para usuários e grupos SMB locais no SVM usando a CLI:

- Se você quiser permitir que membros de um grupo de domínio ou local personalizado ignorem a verificação transversal, você deve adicionar o `SeChangeNotifyPrivilege` privilégio a esse grupo.
- Se você quiser permitir que um usuário local ou de domínio individual ignore a verificação transversal e que o usuário não seja membro de um grupo com esse privilégio, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a essa conta de usuário.
- Você pode desativar a verificação de desvio transversal para usuários ou grupos locais ou de domínio removendo o `SeChangeNotifyPrivilege` privilégio a qualquer momento.

> Para desativar a verificação de desvio de travers para usuários ou grupos locais ou de domínio especificados, você também deve remover o `SeChangeNotifyPrivilege` privilégio do `Everyone` grupo.

Informações relacionadas

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Criar listas de controle de acesso de compartilhamento SMB

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Lista de Privileges suportados

Adicione Privileges a usuários ou grupos locais ou de domínio

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você quiser que um usuário possa percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões em um diretório atravessado, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a usuários ou grupos SMB locais em máquinas virtuais de armazenamento (SVMs). Por padrão, os usuários são capazes de ignorar a verificação de rotação do diretório.

Antes de começar

- Um servidor SMB deve estar presente na SVM.
- A opção local Users and Groups SMB Server (usuários locais e grupos) deve estar ativada.
- O usuário ou grupo local ou domínio ao qual o `SeChangeNotifyPrivilege` privilégio será adicionado já deve existir.

Sobre esta tarefa

Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Ative a verificação de desvio transversal adicionando o `SeChangeNotifyPrivilege` privilégio a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   O valor para o `-user-or-group-name` parâmetro é um usuário ou grupo local, ou um usuário ou grupo de domínio.

2. Verifique se o usuário ou grupo especificado tem a verificação transversal de desvio ativada: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O comando a seguir permite que os usuários que pertencem ao grupo "'EXAMPLE'" ignorem a verificação da rotação do diretório adicionando o `SeChangeNotifyPrivilege` privilégio ao grupo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

Informações relacionadas

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você não quiser que um usuário percorra todos os diretórios no caminho para um arquivo porque o usuário não tem permissões no diretório atravessado, você pode remover o `SeChangeNotifyPrivilege` privilégio de usuários SMB locais ou grupos em máquinas virtuais de armazenamento (SVMs).

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Não permitir a verificação da travessa de derivação: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   O comando remove o `SeChangeNotifyPrivilege` privilégio do usuário ou grupo local ou domínio que você especificar com o valor do `-user-or-group-name` *`name`* parâmetro.

2. Verifique se o usuário ou grupo especificado tem verificação de desvio de rotação desativada: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O comando a seguir despermite que os usuários que pertencem ao grupo "'EXAMPLE"' ignorem a verificação da rotação do diretório:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          -
```

Informações relacionadas

Permitir que usuários ou grupos ignorem a verificação de rotação do diretório

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Exibir informações sobre a visão geral das políticas de auditoria e segurança de arquivos

Você pode exibir informações sobre segurança de arquivos em arquivos e diretórios contidos em volumes em máquinas virtuais de armazenamento (SVMs). Você pode exibir informações sobre políticas de auditoria no FlexVol volumes. Se configurado, você pode exibir informações sobre as configurações de segurança do Guarda de Acesso em nível de armazenamento e Controle Dinâmico de Acesso no FlexVol volumes.

Exibindo informações sobre segurança de arquivos

Você pode exibir informações sobre a segurança de arquivos aplicada a dados contidos em volumes e qtrees (para volumes FlexVol) com os seguintes estilos de segurança:

- NTFS
- UNIX
- Misto

Exibindo informações sobre políticas de auditoria

Você pode exibir informações sobre políticas de auditoria para auditar eventos de acesso em volumes do FlexVol nos seguintes protocolos nas:

- SMB (todas as versões)
- NFSv4.x

Exibindo informações sobre a segurança do Storage-Level Access Guard (SLAG)

A segurança do Access Guard no nível de storage pode ser aplicada em volumes e objetos de qtree do FlexVol com os seguintes estilos de segurança:

- NTFS
- Misto
- UNIX (se um servidor CIFS estiver configurado na SVM que contém o volume)

Apresentar informações sobre a segurança do controlo de acesso dinâmico (DAC)

A segurança do controle de acesso dinâmico pode ser aplicada em um objeto dentro de um FlexVol volume com os seguintes estilos de segurança:

- NTFS
- Misto (se o objeto tiver segurança efetiva NTFS)

Informações relacionadas

Protegendo o acesso aos arquivos usando o Storage-Level Access Guard

Exibindo informações sobre o Storage-Level Access Guard

Exibir informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Você pode exibir informações sobre a segurança de arquivos e diretórios em volumes de estilo de segurança NTFS, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre os atributos dos. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Como os volumes e qtrees de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.
- A saída ACL é exibida para arquivos e pastas com segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada na raiz de volume ou qtree, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir ACLs de arquivo regulares e ACLs de Storage-Level Access Guard.
- A saída também exibe informações sobre os ACEs do Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório específico.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Se você quiser exibir informações…	Digite o seguinte comando…
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/vol4` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança com máscaras expandidas sobre o caminho `/data/engineering` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
```

```
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
```

```
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
```

```
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

O exemplo a seguir exibe informações de segurança, incluindo informações de segurança do Storage-Level Access Guard, para o volume com o caminho `/datavol1` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Exibir informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes mistos de estilo de segurança, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.
- O nível superior de um volume de estilo de segurança misto pode ter segurança eficaz UNIX ou NTFS.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto as permissões de arquivo UNIX quanto as ACLs Storage-Level Access Guard.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho de arquivo ou diretório dado.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/projects` no SVM VS1 no formulário de máscara expandida. Este caminho de estilo de segurança misto tem segurança eficaz UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho `/data` no SVM VS1. Este caminho misto de estilo de segurança tem uma segurança eficaz NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança sobre o volume no caminho `/datavol5` no SVM VS1. O nível superior deste volume misto de estilo de segurança tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Exibir informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes estilo de segurança UNIX, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e

grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou diretório você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 ao determinar direitos de acesso a arquivos.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NFSv4.

  Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída de proprietário e grupo na saída ACL não se aplicam no caso de descritores de segurança NFSv4.

  Eles são apenas significativos para descritores de segurança NTFS.

- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Com detalhes expandidos	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1 no formulário de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibir informações sobre políticas de auditoria NTFS em volumes FlexVol usando a CLI

Você pode exibir informações sobre políticas de auditoria NTFS no FlexVol volumes, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre listas de controle de acesso do sistema. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou pastas cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança NTFS usam apenas as listas de controle de acesso do sistema NTFS (SACLs) para políticas de auditoria.
- Arquivos e pastas em um volume misto de estilo de segurança com segurança efetiva NTFS podem ter políticas de auditoria NTFS aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir tanto o arquivo normal quanto a pasta NFSv4 SACLs e o Storage-Level Access Guard NTFS SACLs.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório fornecido.
- Ao exibir informações de segurança sobre arquivos e pastas com segurança efetiva NTFS, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.

  Arquivos e pastas de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos.

- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.

Passo

1. Exiba as configurações de diretiva de auditoria de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Como uma lista detalhada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações da política de auditoria do caminho `/corp` no SVM VS1. O caminho tem segurança eficaz NTFS. O descritor de segurança NTFS contém uma entrada SACL DE sucesso e uma entrada de sucesso/FALHA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

O exemplo a seguir exibe as informações da política de auditoria do caminho `/datavol1` no SVM VS1. O caminho contém SACLs de arquivo e pasta regulares e SACLs de proteção de acesso em nível de armazenamento.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Exiba informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI

Você pode exibir informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI do ONTAP, incluindo quais são os estilos de segurança e estilos de

segurança eficazes, quais permissões são aplicadas e informações sobre as listas de controle de acesso do sistema (SACLs). Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou diretórios cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas SACLs NFSv4 para políticas de auditoria.
- Arquivos e diretórios em um volume misto de estilo de segurança que são de estilo de segurança UNIX podem ter políticas de auditoria NFSv4 aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NFSv4.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto SACLs de arquivo NFSv4 regulares como de diretório e SACLs de acesso no nível de armazenamento NTFS SACLs.
- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passos

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/lab` no SVM VS1. Este caminho de

estilo de segurança UNIX tem um SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Maneiras de exibir informações sobre segurança de arquivos e diretivas de auditoria

Você pode usar o caractere curinga (*) para exibir informações sobre segurança de arquivos e políticas de auditoria de todos os arquivos e diretórios em um determinado caminho ou volume raiz.

O caractere curinga (**) pode ser usado como o último subcomponente de um determinado caminho de diretório abaixo do qual você deseja exibir informações de todos os arquivos e diretórios. Se você quiser exibir informações de um arquivo ou diretório específico chamado "*"**, então você precisa fornecer o caminho completo dentro de aspas duplas ("*").

Exemplo

O comando a seguir com o caractere curinga exibe as informações sobre todos os arquivos e diretórios abaixo do caminho `/1/` do SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

O comando a seguir exibe as informações de um arquivo chamado "*" no caminho `/vol1/a` do SVM VS1. O caminho está entre aspas duplas (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: “/vol1/a/*”
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 1002
          Unix Group Id: 65533
         Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a CLI

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a visão geral da CLI

Você pode gerenciar a segurança de arquivos NTFS, políticas de auditoria NTFS e o Storage-Level Access Guard em máquinas virtuais de armazenamento (SVMs) usando a CLI.

Você pode gerenciar políticas de segurança e auditoria de arquivos NTFS de clientes SMB ou usando a CLI. No entanto, usar a CLI para configurar políticas de segurança e auditoria de arquivos remove a necessidade de usar um cliente remoto para gerenciar a segurança de arquivos. Usar a CLI pode reduzir significativamente o tempo necessário para aplicar a segurança em muitos arquivos e pastas usando um único comando.

Você pode configurar o Storage-Level Access Guard, que é outra camada de segurança aplicada pelo ONTAP aos volumes SVM. O Storage-Level Access Guard aplica-se a acessos de todos os protocolos nas ao objeto de armazenamento ao qual o Storage-Level Access Guard é aplicado.

O protetor de acesso no nível de storage pode ser configurado e gerenciado somente a partir da CLI do ONTAP. Não é possível gerenciar as configurações do protetor de acesso em nível de armazenamento de clientes SMB. Além disso, se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX). Portanto, o Storage-Level Access Guard fornece uma camada extra de segurança para o acesso aos dados que é definido e gerenciado de forma independente pelo administrador do armazenamento.

Embora apenas as permissões de acesso NTFS sejam suportadas pelo Guarda de Acesso em nível de armazenamento, o ONTAP pode executar verificações de segurança para acesso através de NFS a dados em volumes em que o Guarda de Acesso em nível de armazenamento é aplicado se o utilizador do UNIX mapear para um utilizador do Windows na SVM que possui o volume.

Volumes de estilo de segurança NTFS

Todos os arquivos e pastas contidos em volumes e qtrees de estilo de segurança NTFS têm segurança efetiva NTFS. Você pode usar a `vserver security file-directory` família de comandos para implementar os seguintes tipos de segurança em volumes de estilo de segurança NTFS:

- Permissões de arquivo e políticas de auditoria para arquivos e pastas contidos no volume
- Segurança no nível de armazenamento de acesso Guarda em volumes

Volumes mistos de estilo de segurança

Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que têm segurança efetiva UNIX e usam permissões de arquivos UNIX, bits de modo ou ACLs NFSv4.x e diretivas de auditoria NFSv4.x, e alguns arquivos e pastas que têm segurança efetiva NTFS e usam permissões de arquivos NTFS e políticas de auditoria. Você pode usar a `vserver security file-directory` família de comandos para aplicar os seguintes tipos de segurança a dados mistos de estilo de segurança:

- Permissões de arquivos e diretivas de auditoria para arquivos e pastas com o estilo de segurança eficaz NTFS no volume ou qtree misto
- Proteção de acesso no nível de armazenamento para volumes com o estilo de segurança eficaz NTFS e UNIX

Volumes de estilo de segurança UNIX

Os volumes e qtrees de estilo de segurança UNIX contêm arquivos e pastas que têm segurança efetiva UNIX (bits de modo ou ACLs NFSv4.x). Você deve ter em mente o seguinte se quiser usar a `vserver security file-directory` família de comandos para implementar a segurança em volumes estilo de segurança UNIX:

- A `vserver security file-directory` família de comandos não pode ser usada para gerenciar políticas de segurança e auditoria de arquivos UNIX em volumes e qtrees de estilo de segurança UNIX.
- Você pode usar a `vserver security file-directory` família de comandos para configurar o Storage-Level Access Guard em volumes de estilo de segurança UNIX, desde que o SVM com o volume de destino contenha um servidor CIFS.

Informações relacionadas

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Use casos para usar a CLI para definir a segurança de arquivos e pastas

Como você pode aplicar e gerenciar a segurança de arquivos e pastas localmente sem envolvimento de um cliente remoto, você pode reduzir significativamente o tempo necessário para definir a segurança em massa em um grande número de arquivos ou pastas.

Você pode se beneficiar do uso da CLI para definir a segurança de arquivos e pastas nos seguintes casos de uso:

- Armazenamento de arquivos em grandes ambientes empresariais, como armazenamento de arquivos em diretórios base
- Migração de dados
- Mudança de domínio do Windows
- Padronização de políticas de segurança e auditoria de arquivos em sistemas de arquivos NTFS

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Você precisa estar ciente de certos limites ao usar a CLI para definir a segurança de arquivos e pastas.

- A `vserver security file-directory` família de comandos não suporta a configuração de ACLs NFSv4.

  Você só pode aplicar descritores de segurança NTFS a arquivos e pastas NTFS.

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

Os descritores de segurança contêm as listas de controle de acesso que determinam quais ações um usuário pode executar em arquivos e pastas e o que é auditado quando um usuário acessa arquivos e pastas.

- **Permissões**

  As permissões são permitidas ou negadas pelo proprietário de um objeto e determinam quais ações um objeto (usuários, grupos ou objetos de computador) pode executar em arquivos ou pastas especificados.

- **Descritores de segurança**

  Descritores de segurança são estruturas de dados que contêm informações de segurança que definem permissões associadas a um arquivo ou pasta.

- **Listas de controle de acesso (ACLs)**

  Listas de controle de acesso são as listas contidas em um descritor de segurança que contêm informações sobre quais ações os usuários, grupos ou objetos de computador podem executar no arquivo ou pasta à qual o descritor de segurança é aplicado. O descritor de segurança pode conter os dois tipos de ACLs a seguir:

  - Listas de controle de acesso discricionárias (DACLs)
  - Listas de controle de acesso do sistema (SACLs)

- **Listas de controle de acesso discricionárias (DACLs)**

  As DACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador que têm acesso permitido ou negado para executar ações em arquivos ou pastas. As DACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Listas de controle de acesso do sistema (SACLs)**

  Os SACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador para os quais eventos de auditoria bem-sucedidos ou com falha são registrados. SACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Entradas de Controle de Acesso (ACEs)**

  Os ases são entradas individuais em DACLs ou SACLs:

  - Uma entrada de controle de acesso DACL especifica os direitos de acesso que são permitidos ou negados para usuários, grupos ou objetos de computador específicos.
  - Uma entrada de controle de acesso SACL especifica os eventos de sucesso ou falha a serem registrados ao auditar ações especificadas executadas por determinados usuários, grupos ou objetos de computador.

- * Herança de permissão*

  A herança de permissões descreve como as permissões definidas em descritores de segurança são propagadas para um objeto de um objeto pai. Somente permissões herdáveis são herdadas por objetos filho. Ao definir permissões no objeto pai, você pode decidir se pastas, subpastas e arquivos podem herdá-los com ""aplicar a `this-folder`, `sub-folders` e 'arquivos"".

Informações relacionadas

"Auditoria de SMB e NFS e rastreamento de segurança"

Configurando e aplicando políticas de auditoria a arquivos e pastas NTFS usando a CLI

Diretrizes para a aplicação de políticas de diretório de arquivos que usam usuários locais ou grupos no destino da recuperação de desastres do SVM

Há certas diretrizes que você deve ter em mente antes de aplicar políticas de diretório de arquivos no destino de recuperação de desastres de máquina virtual de armazenamento (SVM) em uma configuração de descarte de ID se a configuração de diretiva de diretório de arquivos usar usuários locais ou grupos no descritor de segurança ou nas entradas DACL ou SACL.

Você pode configurar uma configuração de recuperação de desastre para um SVM em que o SVM de origem no cluster de origem replique os dados e a configuração da SVM de origem a um SVM de destino em um cluster de destino.

É possível configurar um dos dois tipos de recuperação de desastres da SVM:

- Identidade preservada

  Com essa configuração, a identidade do SVM e do servidor CIFS é preservada.

- Identidade descartada

  Com essa configuração, a identidade do SVM e do servidor CIFS não é preservada. Nesse cenário, o nome do SVM e do servidor CIFS no SVM de destino são diferentes do SVM e do nome do servidor CIFS na SVM de origem.

Diretrizes para configurações de identidade descartadas

Em uma configuração de identidade descartada, para uma origem SVM que contenha configurações de usuário, grupo e privilégio locais, o nome do domínio local (nome do servidor CIFS local) deve ser alterado para corresponder ao nome do servidor CIFS no destino SVM. Por exemplo, se o nome do SVM de origem for "'VS1'" e o nome do servidor CIFS for "'CIFS1 user1'", e o nome do SVM de destino for "'VS1 user1_dst'" e o nome do servidor CIFS for "'CIFS1_DST'", então o nome de domínio local para um usuário local chamado "'CIFS1'" é alterado automaticamente para "'CIFS1_DST'" no destino:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Mesmo que os nomes de usuários e grupos locais sejam alterados automaticamente nos bancos de dados de usuários e grupos locais, usuários locais ou nomes de grupos não são alterados automaticamente nas configurações de diretiva de diretório de arquivos (políticas configuradas na CLI usando a `vserver security file-directory` família de comandos).

Por exemplo, para "'VS1'", se você configurou uma entrada DACL onde o `-account` parâmetro é definido como "'CIFS1 " user1'", a configuração não será alterada automaticamente no SVM de destino para refletir o nome do servidor CIFS de destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Você deve usar os `vserver security file-directory modify` comandos para alterar manualmente o nome do servidor CIFS para o nome do servidor CIFS de destino.

Componentes de configuração de diretiva de diretório de arquivos que contêm parâmetros de conta

Há três componentes de configuração de diretiva de diretório de arquivos que podem usar configurações de parâmetros que podem conter usuários ou grupos locais:

- Descritor de segurança

  Opcionalmente, você pode especificar o proprietário do descritor de segurança e o grupo principal do proprietário do descritor de segurança. Se o descritor de segurança usar um usuário ou grupo local para as entradas do proprietário e do grupo primário, você deverá modificar o descritor de segurança para usar o SVM de destino no nome da conta. Você pode usar o `vserver security file-directory ntfs modify` comando para fazer quaisquer alterações necessárias nos nomes de conta.

- Entradas DACL

  Cada entrada DACL deve ser associada a uma conta. Você deve modificar quaisquer DACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o nome da conta para entradas DACL existentes, você deve remover quaisquer entradas DACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas DACL com os nomes de conta de destino corrigidos e associar essas novas entradas DACL aos descritores de segurança apropriados.

- Entradas SACL

  Cada entrada SACL deve ser associada a uma conta. Você deve modificar quaisquer SACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o

nome da conta para entradas SACL existentes, você deve remover quaisquer entradas SACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas SACL com os nomes de conta de destino corrigidos e associar essas novas entradas SACL aos descritores de segurança apropriados.

Você deve fazer as alterações necessárias aos usuários locais ou grupos usados na configuração da diretiva de diretório de arquivos antes de aplicar a diretiva; caso contrário, a tarefa aplicar falha.

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar um descritor de segurança NTFS (política de segurança de arquivos) é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em máquinas virtuais de armazenamento (SVMs). Você pode associar o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Adicione entradas de controle de acesso NTFS DACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) DACL (lista de controle de acesso discricionária) ao descritor de segurança NTFS é a segunda etapa na configuração e aplicação de ACLs NTFS a um arquivo ou pasta. Cada entrada identifica qual objeto é permitido ou negado acesso e define o que o objeto pode ou não pode fazer aos arquivos ou pastas definidos no ACE.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs à DACL do descritor de segurança.

Se o descritor de segurança contiver uma DACL que tenha ACEs existentes, o comando adicionará o novo ACE à DACL. Se o descritor de segurança não contiver uma DACL, o comando criará a DACL e adicionará a nova ACE a ele.

Opcionalmente, você pode personalizar entradas DACL especificando quais direitos deseja permitir ou negar para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)

> Se você não especificar direitos para a entrada DACL, o padrão será definir os direitos como `Full Control`.

Opcionalmente, você pode personalizar entradas DACL especificando como aplicar herança.

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma entrada DACL a um descritor de segurança: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Verifique se a entrada DACL está correta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
           Account Name or SID: DOMAIN\joe
                Access Rights: full-control
        Advanced Access Rights: -
                     Apply To: this-folder
                Access Rights: full-control
```

Crie políticas de segurança

Criar uma política de segurança de arquivos para SVMs é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada SVM (contendo volumes de estilo de segurança NTFS ou volumes de estilo de segurança misto).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contentor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para

um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

  Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

  Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

  Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

Ao adicionar tarefas a políticas de segurança, você deve especificar os quatro parâmetros necessários a seguir:

- Nome do SVM
- Nome da política
- Caminho
- Descritor de segurança para associar ao caminho

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas

de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicar políticas de segurança

Aplicar uma política de segurança de arquivos a SVMs é a última etapa na criação e aplicação de ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).

> Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifique a segurança do arquivo aplicado

Você pode verificar as configurações de segurança do arquivo para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações desejadas.

Sobre esta tarefa

Você deve fornecer o nome do SVM que contém os dados e o caminho para o arquivo e pastas em que deseja verificar as configurações de segurança. Você pode usar o parâmetro opcional `-expand-mask` para exibir informações detalhadas sobre as configurações de segurança.

Passo

1. Exibir configurações de segurança de arquivos e pastas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
```

```
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
```

```
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a visão geral da CLI

Existem várias etapas que você deve executar para aplicar políticas de auditoria a arquivos e pastas NTFS ao usar a CLI do ONTAP. Primeiro, você cria um descritor de segurança NTFS e adiciona SACLs ao descritor de segurança. Em seguida, você cria uma política de segurança e adiciona tarefas de política. Em seguida, você aplica a política de segurança a uma máquina virtual de storage (SVM).

Sobre esta tarefa

Depois de aplicar a política de segurança, pode monitorizar o trabalho de política de segurança e, em seguida, verificar as definições da política de auditoria aplicada.

Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Informações relacionadas

Protegendo o acesso aos arquivos usando o Storage-Level Access Guard

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

"Auditoria de SMB e NFS e rastreamento de segurança"

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar uma política de auditoria do descritor de segurança NTFS é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em SVMs. Você associará o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Se pretender utilizar os parâmetros avançados, defina o nível de privilégio para avançado: `set -privilege advanced`
2. Criar um descritor de segurança: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verifique se a configuração do descritor de segurança está correta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Se estiver no nível de privilégio avançado, regresse ao nível de privilégio admin: `set -privilege admin`

Adicione entradas de controle de acesso NTFS SACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) SACL (lista de controle de acesso do sistema) ao descritor de segurança NTFS é a segunda etapa na criação de políticas de auditoria NTFS para arquivos ou pastas em SVMs. Cada entrada identifica o usuário ou grupo que você deseja auditar. A entrada SACL define se você deseja auditar tentativas de acesso bem-sucedidas ou com falha.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs ao SACL do descritor de segurança.

Se o descritor de segurança contiver um SACL que tenha ACEs existentes, o comando adicionará o novo ACE ao SACL. Se o descritor de segurança não contiver um SACL, o comando criará o SACL e adicionará o novo ACE a ele.

Você pode configurar entradas SACL especificando quais direitos deseja auditar para eventos de sucesso ou falha para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)

Se não especificar direitos para a entrada SACL, a predefinição é `Full Control`.

Opcionalmente, você pode personalizar entradas SACL especificando como aplicar herança com o `apply to` parâmetro. Se você não especificar esse parâmetro, o padrão é aplicar essa entrada SACL a essa pasta, subpastas e arquivos.

Passos

1. Adicione uma entrada SACL a um descritor de segurança: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Verifique se a entrada SACL está correta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                  Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Crie políticas de segurança

Criar uma política de auditoria para máquinas virtuais de armazenamento (SVMs) é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada máquina virtual de armazenamento (SVM) (contendo volumes de estilo de segurança NTFS ou volumes mistos de estilo de segurança).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver`

```
vserver_name -policy-name policy_name

vserver security file-directory policy create -policy-name policy1 -vserver
vs1
```

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contentor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

  Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

  Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

  Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva

deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicar políticas de segurança

Aplicar uma política de auditoria a SVMs é a última etapa na criação e aplicação de

ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).

> Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifique a política de auditoria aplicada

Você pode verificar a política de auditoria para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações de segurança de auditoria desejadas.

Sobre esta tarefa

Você usa o `vserver security file-directory show` comando para exibir informações da política de auditoria. Você deve fornecer o nome do SVM que contém os dados e o caminho para os dados cujas informações de política de auditoria de arquivo ou pasta você deseja exibir.

Passo

1. Exibir configurações da política de auditoria: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Exemplo

O comando a seguir exibe as informações da política de auditoria aplicadas ao caminho "'/corp" no SVM VS1. O caminho tem um SUCESSO e uma entrada SACL DE SUCESSO/FALHA aplicada a ele:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
       Unix Group Id: 0
      Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                  ACLs: NTFS Security Descriptor
                        Control:0x8014
                        Owner:DOMAIN\Administrator
                        Group:BUILTIN\Administrators
                        SACL - ACEs
                          ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                          SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                        DACL - ACEs
                          ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                          ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                          ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerações ao gerenciar trabalhos de diretiva de segurança

Se existir um trabalho de política de segurança, em determinadas circunstâncias, não é possível modificar essa política de segurança ou as tarefas atribuídas a essa diretiva. Você deve entender em que condições você pode ou não pode modificar políticas de segurança para que quaisquer tentativas que você fizer para modificar a diretiva sejam bem-sucedidas. As modificações à política incluem adicionar, remover ou modificar tarefas atribuídas à política e excluir ou modificar a política.

Não é possível modificar uma política de segurança ou uma tarefa atribuída a essa política se existir um trabalho para essa política e essa tarefa estiver nos seguintes estados:

- O trabalho está em execução ou em curso.
- O trabalho está em pausa.
- O trabalho é retomado e está no estado em execução.
- Se a tarefa estiver aguardando o failover para outro nó.

Nas seguintes circunstâncias, se existir um trabalho para uma política de segurança, pode modificar com êxito essa política de segurança ou uma tarefa atribuída a essa política:

- O trabalho de política é interrompido.
- O trabalho de política foi concluído com êxito.

Comandos para gerenciar descritores de segurança NTFS

Existem comandos ONTAP específicos para gerenciar descritores de segurança. Você pode criar, modificar, excluir e exibir informações sobre descritores de segurança.

Se você quiser…	Use este comando…
Crie descritores de segurança NTFS	`vserver security file-directory ntfs create`
Modificar descritores de segurança NTFS existentes	`vserver security file-directory ntfs modify`
Exibir informações sobre descritores de segurança NTFS existentes	`vserver security file-directory ntfs show`
Excluir descritores de segurança NTFS	`vserver security file-directory ntfs delete`

Consulte as páginas de manual para `vserver security file-directory ntfs` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS DACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso

DACL (ACEs). Você pode adicionar ACEs a DACLs NTFS a qualquer momento. Você também pode gerenciar DACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em DACLs.

Se você quiser…	Use este comando…
Crie ACEs e adicione-os a DACLs NTFS	`vserver security file-directory ntfs dacl add`
Modificar ACEs existentes em DACLs NTFS	`vserver security file-directory ntfs dacl modify`
Exibir informações sobre ACEs existentes em DACLs NTFS	`vserver security file-directory ntfs dacl show`
Remover ACEs existentes de DACLs NTFS	`vserver security file-directory ntfs dacl remove`

Consulte as páginas de manual para `vserver security file-directory ntfs dacl` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS SACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso SACL (ACEs). Você pode adicionar ACEs a SACLs NTFS a qualquer momento. Você também pode gerenciar SACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em SACLs.

Se você quiser…	Use este comando…
Crie ACEs e adicione-os a SACLs NTFS	`vserver security file-directory ntfs sacl add`
Modificar ACEs existentes em SACLs NTFS	`vserver security file-directory ntfs sacl modify`
Exibir informações sobre ACEs existentes em SACLs NTFS	`vserver security file-directory ntfs sacl show`
Remover ACEs existentes de SACLs NTFS	`vserver security file-directory ntfs sacl remove`

Consulte as páginas de manual para `vserver security file-directory ntfs sacl` obter mais informações.

Comandos para gerenciar políticas de segurança

Existem comandos ONTAP específicos para gerenciar políticas de segurança. Você pode exibir informações sobre políticas e excluir políticas. Não é possível modificar uma política de segurança.

Se você quiser…	Use este comando…
Crie políticas de segurança	`vserver security file-directory policy create`
Exibir informações sobre políticas de segurança	`vserver security file-directory policy show`
Eliminar políticas de segurança	`vserver security file-directory policy delete`

Consulte as páginas de manual para `vserver security file-directory policy` obter mais informações.

Comandos para gerenciar tarefas de diretiva de segurança

Existem comandos ONTAP para adicionar, modificar, remover e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser…	Use este comando…
Adicione tarefas de política de segurança	`vserver security file-directory policy task add`
Modificar tarefas de política de segurança	`vserver security file-directory policy task modify`
Exibir informações sobre as tarefas da diretiva de segurança	`vserver security file-directory policy task show`
Remover tarefas de política de segurança	`vserver security file-directory policy task remove`

Consulte as páginas de manual para `vserver security file-directory policy task` obter mais informações.

Comandos para gerenciar trabalhos de diretiva de segurança

Existem comandos ONTAP para pausar, retomar, parar e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser…	Use este comando…
Pausar trabalhos de diretiva de segurança	`vserver security file-directory job pause -vserver vserver_name -id integer`
Retomar os trabalhos de política de segurança	`vserver security file-directory job resume -vserver vserver_name -id integer`
Exibir informações sobre os trabalhos de diretiva de segurança	`vserver security file-directory job show -vserver vserver_name` Pode determinar a ID da tarefa de uma tarefa utilizando este comando.
Interromper trabalhos de política de segurança	`vserver security file-directory job stop -vserver vserver_name -id integer`

Consulte as páginas de manual para `vserver security file-directory job` obter mais informações.

Configure o cache de metadados para compartilhamentos SMB

Como o armazenamento em cache de metadados SMB funciona

O armazenamento em cache de metadados permite o armazenamento em cache de atributos de arquivo em clientes SMB 1,0 para fornecer acesso mais rápido aos atributos de arquivo e pasta. Você pode ativar ou desativar o cache de atributos por compartilhamento. Você também pode configurar o tempo de permanência para entradas em cache se o armazenamento em cache de metadados estiver habilitado. A configuração do cache de metadados não é necessária se os clientes estiverem se conetando a compartilhamentos por SMB 2.x ou SMB 3,0.

Quando ativado, o cache de metadados SMB armazena dados de caminho e atributo de arquivo por um período limitado de tempo. Isso pode melhorar a performance do SMB para clientes SMB 1,0 com workloads comuns.

Para certas tarefas, o SMB cria uma quantidade significativa de tráfego que pode incluir várias consultas idênticas para metadados de caminho e arquivo. Você pode reduzir o número de consultas redundantes e melhorar o desempenho para clientes SMB 1,0 usando o cache de metadados SMB para buscar informações do cache.

> Embora improvável, é possível que o cache de metadados possa servir informações obsoletas para clientes SMB 1,0. Se o seu ambiente não puder suportar esse risco, você não deve habilitar esse recurso.

Ative o cache de metadados SMB

Você pode melhorar o desempenho do SMB para clientes SMB 1,0 ativando o cache de metadados SMB. Por padrão, o armazenamento em cache de metadados SMB está desativado.

Passo

1. Execute a ação desejada:

Se você quiser…	Digite o comando…
Ative o armazenamento em cache de metadados SMB ao criar um compartilhamento	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache`
Habilite o armazenamento em cache de metadados SMB em um compartilhamento existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Informações relacionadas

Configurando o tempo de vida das entradas de cache de metadados SMB

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Configure o tempo de vida das entradas de cache de metadados SMB

Você pode configurar o tempo de vida das entradas de cache de metadados SMB para otimizar o desempenho do cache de metadados SMB em seu ambiente. O padrão é 10 segundos.

Antes de começar

Você deve ter habilitado o recurso de cache de metadados SMB. Se o armazenamento em cache de metadados SMB não estiver ativado, a configuração TTL de cache SMB não será usada.

Passo

1. Execute a ação desejada:

Se você quiser configurar o tempo de vida das entradas de cache de metadados SMB quando…	Digite o comando…
Crie um compartilhamento	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modificar um compartilhamento existente	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

Você pode especificar opções e propriedades de configuração de compartilhamento adicionais ao criar ou modificar compartilhamentos. Consulte as páginas de manual para obter mais informações.

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm` , `rmdir` e `mv` podem causar falha no aplicativo NFS.
- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB deny-read e deny-write, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um bytelock SMB exclusivo.
- Desvincular
  - Para sistemas de arquivos NTFS, as operações de exclusão SMB e CIFS são suportadas.

    O arquivo será removido após o último fechamento.
  - As operações de desvinculação NFS não são suportadas.

    Ele não é suportado porque as semânticas NTFS e SMB são necessárias e a última operação Excluir-em-close não é suportada para NFS.
  - Para sistemas de arquivos UNIX, a operação de desvinculação é suportada.

    Ele é compatível porque a semântica NFS e UNIX são necessárias.
- Mudar o nome
  - Para sistemas de arquivos NTFS, se o arquivo de destino for aberto a partir de SMB ou CIFS, o arquivo de destino pode ser renomeado.
  - O nome de NFS não é suportado.

    Não é suportado porque as semânticas NTFS e SMB são necessárias.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.
- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.

> As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança que impedem que usuários ou aplicativos renomeem diretórios críticos.

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4,1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.
- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho . O modo de acesso sharelock é write-deny_none, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de write-deny_none para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
```

```
                Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
            Lock Protocol: cifs
                Lock Type: share-level
   Node Holding Lock State: node3
              Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
        SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
                   Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/test.pptx
                Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
            Lock Protocol: cifs
                Lock Type: op-lock
   Node Holding Lock State: node3
              Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
        SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
```

```
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Bloqueios de rutura

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

   A página de manual do comando contém informações detalhadas.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Execute uma das seguintes ações:

Se você quiser quebrar um bloqueio especificando…	Digite o comando…
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
A ID de bloqueio	`vserver locks break -lockid UUID`

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Monitorar a atividade de SMB

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

  Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB…	**Digite o seguinte comando…**
Para todas as sessões no SVM de forma resumida	`vserver cifs session show -vserver vserver_name`
Em um ID de conexão especificado	`vserver cifs session show -vserver vserver_name -connection-id integer`
A partir de um endereço IP de estação de trabalho especificado	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Em um endereço IP de LIF especificado	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Em um nó especificado	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	De um usuário do Windows especificado
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Com um mecanismo de autenticação especificado
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Com uma versão de protocolo especificada	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
SMB3	SMB3_1}`  [NOTE] ==== A proteção continuamente disponível e o SMB multicanal estão disponíveis apenas nas sessões SMB 3,0 e posteriores. Para ver o seu estado em todas as sessões de qualificação, deve especificar este parâmetro com o valor definido para `SMB3` ou posterior. ====
Com um nível especificado de proteção continuamente disponível	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Se o status continuamente disponível for `Partial`, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode usar o `vserver cifs sessions file show` comando para determinar quais arquivos na sessão estabelecida não estão abertos com proteção continuamente disponível. ====
Com um status de sessão de assinatura SMB especificado	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço IP 10,1.1,1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conetado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conetar com a proteção continuamente disponível.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informações relacionadas

Exibindo informações sobre arquivos SMB abertos

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show`

comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
No SVM no formulário de resumo	`vserver cifs session file show -vserver vserver_name`
Em um nó especificado	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	Em um ID de arquivo especificado
`vserver cifs session file show -vserver vserver_name -file-id integer`	Em uma ID de conexão SMB especificada
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Em um SMB Session ID especificado
`vserver cifs session file show -vserver vserver_name -session-id integer`	No agregado de hospedagem especificado
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	No volume especificado
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	No compartilhamento SMB especificado

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	No caminho SMB especificado
`vserver cifs session file show -vserver vserver_name -path path`	Com o nível especificado de proteção continuamente disponível
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Se o status continuamente disponível for `No`, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade. ====
Com o estado de reconexão especificado	`vserver cifs session file show -vserver vserver_name -reconnected {No

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informações relacionadas

Exibindo informações de sessão SMB

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser determinar…	Digite…
Quais objetos estão disponíveis	`statistics catalog object show`
Objetos específicos que estão disponíveis	`statistics catalog object show object object_name`
Quais contadores estão disponíveis	`statistics catalog counter show object object_name`

   Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível de privilégio avançado:

Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informações relacionadas

Exibindo estatísticas

Apresentar estatísticas

É possível exibir várias estatísticas, incluindo estatísticas sobre CIFS e SMB, auditoria e hashes BranchCache, para monitorar a performance e diagnosticar problemas.

Antes de começar

Você deve ter coletado amostras de dados usando os `statistics start` comandos e `statistics stop` antes de exibir informações sobre objetos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser exibir estatísticas para…	Digite…
Todas as versões do SMB	`statistics show -object cifs`
SMB 1,0	`statistics show -object smb1`
SMB 2.x e SMB 3,0	`statistics show -object smb2`
Subsistema CIFS do nó	`statistics show -object nblade_cifs`
Auditoria multiprotocolo	`statistics show -object audit_ng`
Serviço de hash BranchCache	`statistics show -object hashd`
DNS dinâmico	`statistics show -object ddns_update`

   Consulte a página de manual de cada comando para obter mais informações.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Determinando quais objetos e contadores de estatísticas estão disponíveis

Monitoramento de estatísticas de sessão assinadas pelo SMB

Exibindo estatísticas do BranchCache

Uso de estatísticas para monitorar a atividade automática de referência de nós

"Configuração SMB para Microsoft Hyper-V e SQL Server"

"Configuração do monitoramento de desempenho"

Implantar serviços baseados em cliente SMB

Use arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Use arquivos off-line para permitir o armazenamento em cache de arquivos para visão geral de uso off-line

O ONTAP suporta o recurso arquivos off-line da Microsoft, ou *cache do lado do cliente*, que permite que os arquivos sejam armazenados em cache no host local para uso off-line. Os usuários podem usar a funcionalidade de arquivos off-line para continuar trabalhando em arquivos, mesmo quando eles são desconetados da rede.

Você pode especificar se os documentos e programas do usuário do Windows são automaticamente armazenados em cache em um compartilhamento ou se os arquivos devem ser selecionados manualmente para armazenamento em cache. O armazenamento em cache manual é ativado por padrão para novos compartilhamentos. Os arquivos disponibilizados offline são sincronizados com o disco local do cliente Windows. A sincronização ocorre quando a conetividade de rede a um compartilhamento de sistema de armazenamento específico é restaurada.

Como os arquivos e pastas offline mantêm as mesmas permissões de acesso que a versão dos arquivos e pastas salvos no servidor CIFS, o usuário deve ter permissões suficientes nos arquivos e pastas salvos no servidor CIFS para executar ações nos arquivos e pastas offline.

Quando o usuário e outra pessoa na rede fazem alterações no mesmo arquivo, o usuário pode salvar a versão local do arquivo na rede, manter a outra versão ou salvar ambas. Se o usuário mantiver ambas as versões, um novo arquivo com as alterações do usuário local será salvo localmente e o arquivo em cache será substituído por alterações da versão do arquivo salvo no servidor CIFS.

Você pode configurar arquivos off-line em uma base de compartilhamento por compartilhamento usando as configurações de compartilhamento. Você pode escolher uma das quatro configurações de pastas offline ao criar ou modificar compartilhamentos:

- Sem armazenamento em cache

  Desativa o cache do lado do cliente para o compartilhamento. Arquivos e pastas não são automaticamente armazenados em cache localmente em clientes e os usuários não podem optar por armazenar em cache arquivos ou pastas localmente.

- Armazenamento manual em cache

  Permite a seleção manual de arquivos a serem armazenados em cache no compartilhamento. Esta é a configuração padrão. Por padrão, nenhum arquivo ou pasta é armazenado em cache no cliente local. Os usuários podem escolher quais arquivos e pastas desejam armazenar em cache localmente para uso off-line.

- Armazenamento automático de documentos

  Permite que os documentos do usuário sejam automaticamente armazenados em cache no compartilhamento. Somente arquivos e pastas acessados são armazenados em cache localmente.

- Armazenamento em cache automático do programa

  Permite que programas e documentos do usuário sejam automaticamente armazenados em cache no compartilhamento. Somente arquivos, pastas e programas acessados são armazenados em cache localmente. Além disso, essa configuração permite que o cliente execute executáveis armazenados

localmente em cache, mesmo quando conetado à rede.

Para obter mais informações sobre a configuração de arquivos off-line em servidores e clientes do Windows, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

Usando perfis de roaming para armazenar perfis de usuário centralmente em um servidor CIFS associado ao SVM

Usando redirecionamento de pasta para armazenar dados em um servidor CIFS

Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos para usar arquivos off-line

Antes de poder utilizar a funcionalidade ficheiros offline da Microsoft com o servidor CIFS, tem de saber quais as versões do ONTAP e SMB e quais os clientes do Windows que suportam a funcionalidade.

Requisitos de versão do ONTAP

As versões do ONTAP suportam arquivos off-line.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP oferece suporte a arquivos off-line em todas as versões do SMB.

Requisitos do cliente Windows

O cliente Windows deve suportar os arquivos off-line.

Para obter as informações mais recentes sobre quais clientes do Windows oferecem suporte ao recurso arquivos off-line, consulte Matriz de interoperabilidade.

"mysupport.NetApp.com/matrix"

Diretrizes para a implantação de arquivos offline

Existem algumas diretrizes importantes que você precisa entender quando você implantar arquivos off-line em compartilhamentos de diretório home que têm a `showsnapshot` propriedade de compartilhamento definida em diretórios home.

Se a `showsnapshot` propriedade compartilhar estiver definida em um compartilhamento de diretório inicial que tenha arquivos off-line configurados, os clientes do Windows armazenam em cache todas as cópias Snapshot `~snapshot` na pasta no diretório inicial do usuário.

Os clientes Windows armazenam em cache todas as cópias Snapshot no diretório inicial se uma das seguintes opções for verdadeira:

- O usuário torna o diretório home disponível offline a partir do cliente.

O conteúdo da `~snapshot` pasta no diretório inicial é incluído e disponibilizado offline.

- O usuário configura o redirecionamento de pasta para redirecionar uma pasta, como `My Documents` a raiz de um diretório home que reside no compartilhamento do servidor CIFS.

  Alguns clientes do Windows podem tornar a pasta redirecionada automaticamente disponível offline. Se a pasta for redirecionada para a raiz do diretório inicial, a `~snapshot` pasta será incluída no conteúdo offline em cache.

> Implantações de arquivos offline onde a `~snapshot` pasta está incluída em arquivos offline devem ser evitadas. As cópias Snapshot na `~snapshot` pasta contêm todos os dados no volume no ponto em que o ONTAP criou a cópia Snapshot. Portanto, criar uma cópia off-line da `~snapshot` pasta consome armazenamento local significativo no cliente, consome largura de banda da rede durante a sincronização de arquivos off-line e aumenta o tempo necessário para sincronizar arquivos off-line.

Configure o suporte a arquivos off-line em compartilhamentos SMB usando a CLI

Você pode configurar o suporte a arquivos off-line usando a CLI do ONTAP especificando uma das quatro configurações de arquivos off-line ao criar compartilhamentos SMB ou a qualquer momento modificando compartilhamentos SMB existentes. O suporte manual de arquivos offline é a configuração padrão.

Sobre esta tarefa

Ao configurar o suporte a arquivos off-line, você pode escolher uma das quatro configurações de arquivos off-line a seguir:

Definição	Descrição
`none`	Não permite que os clientes Windows armazenem quaisquer arquivos neste compartilhamento.
`manual`	Permite que os usuários em clientes Windows selecionem manualmente os arquivos a serem armazenados em cache.
`documents`	Permite que os clientes Windows armazenem documentos de usuário que são usados pelo usuário para acesso off-line.
`programs`	Permite que os clientes do Windows armazenem programas que são usados pelo usuário para acesso off-line. Os clientes podem usar os arquivos de programa armazenados em cache no modo offline, mesmo que o compartilhamento esteja disponível.

Você pode escolher apenas uma configuração de arquivo off-line. Se você modificar uma configuração de arquivos off-line em um compartilhamento SMB existente, a nova configuração arquivos off-line substituirá a configuração original. Outras configurações de compartilhamento SMB existentes e propriedades de compartilhamento não são removidas ou substituídas. Eles permanecem em vigor até que sejam

explicitamente removidos ou alterados.

Passos

1. Execute a ação apropriada:

Se você quiser configurar arquivos off-line em…	Digite o comando…
Um novo compartilhamento SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Um compartilhamento SMB existente
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Verifique se a configuração do compartilhamento SMB está correta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemplo

O comando a seguir cria um compartilhamento SMB chamado "d.ATA1" com arquivos off-line definidos como `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                  Share Comment: Offline files
                      Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                  Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

O comando a seguir modifica um compartilhamento SMB existente chamado "d.ATA1" alterando a configuração de arquivos off-line `manual` e adicionando valores para a máscara de criação de modo de arquivo e diretório:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informações relacionadas

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Configure o suporte a arquivos off-line em compartilhamentos SMB usando o MMC Gerenciamento do computador

Se você quiser permitir que os usuários armazenem arquivos localmente para uso off-line, você pode configurar o suporte a arquivos off-line usando o MMC de Gerenciamento do computador (Microsoft Management Console).

Passos

1. Para abrir o MMC no servidor Windows, no Windows Explorer, clique com o botão direito do Mouse no ícone do computador local e selecione **Gerenciar**.
2. No painel esquerdo, selecione **Gerenciamento de computador**.
3. Selecione **Ação** > **ligar a outro computador**.

   A caixa de diálogo Selecionar computador é exibida.

4. Digite o nome do servidor CIFS ou clique em **Procurar** para localizar o servidor CIFS.

   Se o nome do servidor CIFS for o mesmo nome do host da máquina virtual de storage (SVM), digite o nome do SVM. Se o nome do servidor CIFS for diferente do nome do host SVM, digite o nome do servidor CIFS.

5. Clique em **OK**.
6. Na árvore da consola, clique em **Ferramentas do sistema** > **pastas partilhadas**.
7. Clique em **compartilhamentos**.
8. No painel de resultados, clique com o botão direito do rato no partilhar.
9. Clique em **Propriedades**.

   As propriedades para a partilha selecionada são apresentadas.

10. Na guia **Geral**, clique em **Configurações off-line**.

    A caixa de diálogo Configurações off-line é exibida.

11. Configure as opções de disponibilidade off-line conforme apropriado.
12. Clique em **OK**.

Use perfis de roaming para armazenar perfis de usuário centralmente em um servidor SMB associado ao SVM

Use perfis de roaming para armazenar perfis de usuário centralmente em um servidor SMB associado à visão geral da SVM

O ONTAP suporta o armazenamento de perfis de roaming do Windows em um servidor CIFS associado à máquina virtual de armazenamento (SVM). A configuração de perfis de roaming de usuários oferece vantagens para o usuário, como disponibilidade automática de recursos, independentemente de onde o usuário faz login. Os perfis de roaming também simplificam a administração e o gerenciamento de perfis de usuário.

Os perfis de usuário de roaming têm as seguintes vantagens:

- Disponibilidade automática de recursos

  O perfil exclusivo de um usuário fica automaticamente disponível quando esse usuário faz login em qualquer computador na rede que esteja executando o Windows 8, Windows 7, Windows 2000 ou Windows XP. Os usuários não precisam criar um perfil em cada computador que usam em uma rede.

- Substituição simplificada do calculador

  Como todas as informações de perfil do usuário são mantidas separadamente na rede, o perfil de um usuário pode ser facilmente baixado em um novo computador de substituição. Quando o usuário faz login no novo computador pela primeira vez, a cópia do perfil do usuário é copiada para o novo computador.

Informações relacionadas

Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Usando redirecionamento de pasta para armazenar dados em um servidor CIFS

Requisitos para usar perfis de roaming

Antes de poder utilizar os perfis de roaming da Microsoft com o seu servidor CIFS, tem de saber quais versões do ONTAP e SMB e quais clientes do Windows suportam a funcionalidade.

Requisitos de versão do ONTAP

ONTAP suporta perfis de roaming.

Requisitos de versão do protocolo SMB

Para máquina virtual de armazenamento (SVM), o ONTAP oferece suporte a perfis de roaming em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar os perfis de roaming, o cliente Windows deve suportar o recurso.

Para obter as informações mais recentes sobre quais clientes Windows suportam perfis de roaming, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Configurar perfis de roaming

Se você quiser disponibilizar automaticamente o perfil de um usuário quando ele fizer logon em qualquer computador da rede, poderá configurar perfis de roaming através do snap-in MMC usuários e computadores do ative Directory. Se estiver configurando perfis de roaming no Windows Server, você poderá usar o Centro de Administração do ative Directory.

Passos

1. No servidor Windows, abra o MMC usuários e computadores do ative Directory (ou o Centro de Administração do ative Directory em servidores Windows).
2. Localize o usuário para o qual você deseja configurar um perfil de roaming.
3. Clique com o botão direito do rato no utilizador e clique em **Propriedades**.
4. Na guia **Perfil**, insira o caminho do perfil para o compartilhamento onde deseja armazenar o perfil de roaming do usuário, seguido de `%username%`.

   Por exemplo, um caminho de perfil pode ser o seguinte `\\vs1.example.com\profiles\%username%`: . A primeira vez que um utilizador inicia sessão `%username%` é substituído pelo nome do utilizador.

   > No caminho `\\vs1.example.com\profiles\%username%` `profiles` , é o nome de compartilhamento de um compartilhamento na máquina virtual de armazenamento (SVM) VS1 que tem direitos de controle total para todos.

5. Clique em **OK**.

Use o redirecionamento de pastas para armazenar dados em um servidor SMB

Use o redirecionamento de pastas para armazenar dados em uma visão geral do servidor SMB

O ONTAP oferece suporte ao redirecionamento de pastas da Microsoft, o que permite que usuários ou administradores redirecionem o caminho de uma pasta local para um local no servidor CIFS. Aparece como se as pastas redirecionadas fossem armazenadas

no cliente Windows local, mesmo que os dados estejam armazenados em um compartilhamento SMB.

O redirecionamento de pastas destina-se principalmente a organizações que já implantaram diretórios base e que desejam manter a compatibilidade com seu ambiente de diretório base existente.

- `Documents`, `Desktop` e `Start Menu` são exemplos de pastas que podem ser redirecionadas.
- Os usuários podem redirecionar pastas de seu cliente Windows.
- Os administradores podem configurar e gerenciar centralmente o redirecionamento de pastas configurando GPOs no ative Directory.
- Se os administradores tiverem configurado perfis de roaming, o redirecionamento de pastas permite que os administradores dividam os dados do usuário dos dados do perfil.
- Os administradores podem usar o redirecionamento de pastas e arquivos offline juntos para redirecionar o armazenamento de dados para pastas locais para o servidor CIFS, permitindo que os usuários armazenem o conteúdo localmente.

Informações relacionadas

Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Usando perfis de roaming para armazenar perfis de usuário centralmente em um servidor CIFS associado ao SVM

Requisitos para usar o redirecionamento de pastas

Antes de poder usar o redirecionamento de pastas da Microsoft com o servidor CIFS, você precisa saber quais versões do ONTAP e SMB e quais clientes do Windows suportam o recurso.

Requisitos de versão do ONTAP

O ONTAP suporta redirecionamento de pastas da Microsoft.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP oferece suporte ao redirecionamento de pastas da Microsoft em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar o redirecionamento de pastas da Microsoft, o cliente do Windows deve suportar o recurso.

Para obter as informações mais recentes sobre quais clientes do Windows suportam redirecionamento de pastas, consulte Matriz de interoperabilidade.

"mysupport.NetApp.com/matrix"

Configurar redirecionamento de pastas

Você pode configurar o redirecionamento de pastas usando a janela Propriedades do Windows. A vantagem de usar esse método é que o usuário do Windows pode

configurar o redirecionamento de pastas sem a ajuda do administrador SVM.

Passos

1. No Explorador do Windows, clique com o botão direito do rato na pasta que pretende redirecionar para uma partilha de rede.
2. Clique em **Propriedades**.

   As propriedades para a partilha selecionada são apresentadas.

3. Na guia **atalho**, clique em **destino** e especifique o caminho para o local da rede onde deseja redirecionar a pasta selecionada.

   Por exemplo, se você quiser redirecionar uma pasta para a `data` pasta em um diretório inicial mapeado para `Q:\`, especifique `Q:\data` como destino.

4. Clique em **OK**.

   Para obter mais informações sobre como configurar pastas offline, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Acesse o diretório de snapshot de clientes Windows usando SMB 2.x

O método usado para acessar o `~snapshot` diretório de clientes do Windows usando SMB 2.x difere do método usado para SMB 1,0. Você precisa entender como acessar o `~snapshot` diretório ao usar conexões SMB 2.x para acessar com êxito os dados armazenados em cópias Snapshot.

O administrador do SVM controla se os usuários em clientes Windows podem exibir e acessar o `~snapshot` diretório em um compartilhamento ativando ou desativando a `showsnapshot` propriedade de compartilhamento usando comandos das famílias de propriedades de compartilhamento cifs do vserver.

Quando a `showsnapshot` propriedade compartilhar está desativada, um usuário em um cliente Windows que usa SMB 2.x não pode exibir o `~snapshot` diretório e não pode acessar cópias Snapshot dentro `~snapshot` do diretório, mesmo quando manualmente inserir o caminho para `~snapshot` o diretório ou para cópias Snapshot específicas dentro do diretório.

Quando a `showsnapshot` propriedade compartilhar está ativada, um usuário em um cliente Windows que usa SMB 2.x ainda não pode exibir o `~snapshot` diretório na raiz do compartilhamento ou em qualquer junção ou diretório abaixo da raiz do compartilhamento. No entanto, depois de se conetar a um compartilhamento, o usuário pode acessar o diretório oculto `~snapshot` anexando manualmente `\~snapshot` ao final do caminho de compartilhamento. O diretório oculto `~snapshot` é acessível a partir de dois pontos de entrada:

- Na raiz da partilha
- Em cada ponto de junção no espaço de partilha

O diretório oculto `~snapshot` não é acessível a partir de subdiretórios que não sejam de junção dentro do compartilhamento.

Exemplo

Com a configuração mostrada no exemplo a seguir, um usuário em um cliente Windows com uma conexão SMB 2.x ao compartilhamento "'eng'" pode acessar o `~snapshot` diretório anexando manualmente `\~snapshot` o caminho de compartilhamento na raiz do compartilhamento e em cada ponto de junção no caminho. O diretório oculto `~snapshot` é acessível a partir dos seguintes três caminhos:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recupere arquivos e pastas usando versões anteriores

Recupere arquivos e pastas usando a visão geral das versões anteriores

A capacidade de usar as versões anteriores da Microsoft é aplicável a sistemas de arquivos que suportam cópias Snapshot de alguma forma e as habilitam. A tecnologia Snapshot faz parte integrante do ONTAP. Os usuários podem recuperar arquivos e pastas de cópias Snapshot de seu cliente Windows usando o recurso versões anteriores da Microsoft.

A funcionalidade de versões anteriores fornece um método para os usuários navegarem pelas cópias Snapshot ou restaurarem dados de uma cópia Snapshot sem a intervenção do administrador de storage. As versões anteriores não são configuráveis. Está sempre ativado. Se o administrador de storage disponibilizar cópias Snapshot em um compartilhamento, o usuário poderá usar versões anteriores para executar as seguintes tarefas:

- Recuperar arquivos que foram excluídos acidentalmente.
- Recuperar de acidentalmente sobrescrever um arquivo.
- Compare versões do arquivo enquanto trabalha.

Os dados armazenados nas cópias Snapshot são somente leitura. Os usuários devem salvar uma cópia de

um arquivo em outro local para fazer quaisquer alterações no arquivo. As cópias snapshot são excluídas periodicamente; portanto, os usuários precisam criar cópias de arquivos contidos em versões anteriores se quiserem manter indefinidamente uma versão anterior de um arquivo.

Requisitos para usar versões anteriores da Microsoft

Antes de poder utilizar versões anteriores com o seu servidor CIFS, precisa de saber quais as versões do ONTAP e SMB e quais os clientes do Windows que o suportam. Você também precisa saber sobre o requisito de configuração de cópia Snapshot.

Requisitos de versão do ONTAP

Suporta versões anteriores.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP é compatível com versões anteriores em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar versões anteriores para acessar dados em cópias Snapshot, o cliente do Windows deve oferecer suporte ao recurso.

Para obter as informações mais recentes sobre quais clientes Windows suportam versões anteriores, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos para configurações de cópia Snapshot

Para usar versões anteriores para acessar dados em cópias Snapshot, uma política de Snapshot habilitada deve estar associada ao volume que contém os dados, os clientes precisam ter acesso aos dados do Snapshot e as cópias Snapshot devem existir.

Use a guia versões anteriores para exibir e gerenciar dados de cópia Snapshot

Os usuários em máquinas clientes Windows podem usar a guia versões anteriores na janela Propriedades do Windows para restaurar dados armazenados em cópias Snapshot sem precisar envolver o administrador da máquina virtual de armazenamento (SVM).

Sobre esta tarefa

Você só poderá usar a guia versões anteriores para exibir e gerenciar dados em cópias Snapshot de dados armazenados no SVM se o administrador tiver habilitado cópias Snapshot no volume que contém o compartilhamento e se o administrador configurar o compartilhamento para mostrar cópias Snapshot.

Passos

1. No Windows Explorer, exiba o conteúdo da unidade mapeada dos dados armazenados no servidor CIFS.
2. Clique com o botão direito do rato no ficheiro ou pasta na unidade de rede mapeada cujas cópias Snapshot pretende visualizar ou gerir.
3. Clique em **Propriedades**.

As propriedades para o arquivo ou pasta selecionado são exibidas.

4. Clique no separador **versões anteriores**.

   Uma lista de cópias Snapshot disponíveis do arquivo ou pasta selecionado é exibida na caixa versões da pasta:. As cópias Snapshot listadas são identificadas pelo prefixo do nome da cópia Snapshot e pelo carimbo de data/hora da criação.

5. Na caixa **versões da pasta:**, clique com o botão direito do Mouse na cópia do arquivo ou pasta que você deseja gerenciar.
6. Execute a ação apropriada:

Se você quiser…	Faça o seguinte…
Exibir dados dessa cópia Snapshot	Clique em **abrir**.
Crie uma cópia dos dados dessa cópia Snapshot	Clique em **Copiar**.

   Os dados nas cópias Snapshot são somente leitura. Se você quiser fazer modificações nos arquivos e pastas listados na guia versões anteriores, salve uma cópia dos arquivos e pastas que deseja modificar para um local gravável e faça modificações nas cópias.

7. Depois de concluir o gerenciamento dos dados do Snapshot, feche a caixa de diálogo **Propriedades** clicando em **OK**.

   Para obter mais informações sobre como usar a guia versões anteriores para exibir e gerenciar dados do Snapshot, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Determine se as cópias Snapshot estão disponíveis para uso em versões anteriores

Você pode exibir cópias Snapshot da guia versões anteriores somente se uma política de snapshot habilitada for aplicada ao volume que contém o compartilhamento e se a configuração de volume permitir acesso a cópias snapshot. Determinar a disponibilidade da cópia Snapshot é útil ao ajudar um usuário com acesso a versões anteriores.

Passos

1. Determine se o volume no qual residem os dados de compartilhamento tem cópias automáticas do Snapshot ativadas e se os clientes têm acesso aos diretórios do Snapshot: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   A saída exibe a política Snapshot associada ao volume, se o acesso ao diretório Snapshot do cliente está habilitado e o número de cópias Snapshot disponíveis.

2. Determine se a política de snapshot associada está ativada: `volume snapshot policy show -policy policy-name`
3. Listar as cópias Snapshot disponíveis: `volume snapshot show -volume volume_name`

Para obter mais informações sobre como configurar e gerenciar políticas de Snapshot e programações de snapshot, "Proteção de dados"consulte .

Exemplo

O exemplo a seguir exibe informações sobre políticas de Snapshot associadas ao volume chamado "ATA1" que contém os dados compartilhados e as cópias Snapshot disponíveis no "ATA1".

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                     3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                SnapMirror Label
    ---------------- -----     --------------------- -------------------
    hourly               6     hourly                -
    daily                2     daily                 daily
    weekly               2     weekly                weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Informações relacionadas

Criando uma configuração Snapshot para habilitar o acesso a versões anteriores

"Proteção de dados"

Crie uma configuração Snapshot para habilitar o acesso a versões anteriores

A funcionalidade de versões anteriores está sempre disponível, desde que o acesso do cliente às cópias Snapshot esteja habilitado e desde que existam cópias Snapshot. Se a configuração da cópia Snapshot não atender a esses requisitos, você poderá criar uma configuração de cópia Snapshot correspondente.

Passos

1. Se o volume que contém o compartilhamento ao qual você deseja permitir o acesso a versões anteriores não tiver uma política Snapshot associada, associe uma política Snapshot ao volume e ative-a usando o `volume modify` comando.

   Para obter mais informações sobre como usar o `volume modify` comando, consulte as páginas de manual.

2. Habilite o acesso às cópias Snapshot usando o `volume modify` comando para definir a `-snap-dir` opção como `true`.

   Para obter mais informações sobre como usar o `volume modify` comando, consulte as páginas de manual.

3. Verifique se as políticas Snapshot estão ativadas e se o acesso aos diretórios Snapshot está ativado usando os `volume show` comandos e. `volume snapshot policy show`

   Para obter mais informações sobre como usar os `volume show` comandos e `volume snapshot policy show`, consulte as páginas de manual.

   Para obter mais informações sobre como configurar e gerenciar políticas de Snapshot e programações de snapshot, "Proteção de dados"consulte .

Informações relacionadas

"Proteção de dados"

Diretrizes para restaurar diretórios que contêm junções

Existem certas diretrizes que você deve ter em mente ao usar versões anteriores para restaurar pastas que contêm pontos de junção.

Ao usar versões anteriores para restaurar pastas com pastas filhas que são pontos de junção, a restauração pode falhar com um `Access Denied` erro.

Você pode determinar se a pasta que você está tentando restaurar contém uma junção usando o `vol show` comando com a `-parent` opção. Você também pode usar os `vserver security trace` comandos para criar logs detalhados sobre problemas de acesso a arquivos e pastas.

Informações relacionadas

Criação e gerenciamento de volumes de dados em namespaces nas

Implante serviços baseados em servidor SMB

Gerenciar diretórios base

Como o ONTAP ativa diretórios base dinâmicos

Os diretórios iniciais do ONTAP permitem configurar um compartilhamento SMB que mapeia para diferentes diretórios com base no usuário que se coneta a ele e um conjunto de variáveis. Em vez de criar compartilhamentos separados para cada usuário, você pode configurar um compartilhamento com alguns parâmetros do diretório inicial para definir a relação de um usuário entre um ponto de entrada (o compartilhamento) e o diretório inicial (um diretório no SVM).

Um usuário que está conetado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários. Existem quatro variáveis que determinam como um usuário é mapeado para um diretório:

- **Nome da partilha**

  Este é o nome do compartilhamento que você cria ao qual o usuário se coneta. Você deve definir a propriedade do diretório base para esse compartilhamento.

  O nome do compartilhamento pode usar os seguintes nomes dinâmicos:

  - `%w` (O nome de utilizador do Windows do utilizador)
  - `%d` (O nome de domínio do Windows do utilizador)
  - `%u` (O nome de usuário UNIX mapeado do usuário) para tornar o nome de compartilhamento exclusivo em todos os diretórios base, o nome de compartilhamento deve conter a/`%w` variável ou `%u`. O nome do compartilhamento pode conter tanto a `%d` e a/`%w` variável (por exemplo, `%d`/`%w`), ou o nome do compartilhamento pode conter uma porção estática e uma porção variável (por exemplo, Home_/`%w`).
- **Caminho de compartilhamento**

  Este é o caminho relativo, que é definido pelo compartilhamento e, portanto, está associado a um dos nomes de compartilhamento, que é anexado a cada caminho de pesquisa para gerar o caminho do diretório home inteiro do usuário a partir da raiz do SVM. Pode ser estático (por exemplo, `home`), dinâmico (por exemplo, `%w`) ou uma combinação dos dois (por exemplo, `eng/%w`).
- **Pesquisar caminhos**

  Esse é o conjunto de caminhos absolutos da raiz do SVM que você especifica que direciona a busca do ONTAP por diretórios base. Você pode especificar um ou mais caminhos de pesquisa usando o `vserver cifs home-directory search-path add` comando. Se você especificar vários caminhos de pesquisa, o ONTAP os tentará na ordem especificada até encontrar um caminho válido.
- **Diretório**

  Este é o diretório home do usuário que você cria para o usuário. O nome do diretório é geralmente o nome do usuário. Você deve criar o diretório home em um dos diretórios que são definidos pelos caminhos de pesquisa.

Como exemplo, considere a seguinte configuração:

- Usuário: John Smith

- Domínio de usuário: acme
- Nome de usuário: jsmith
- Nome do SVM: VS1
- Nome de compartilhamento de diretório base nº 1: Home_ `%w` - caminho de compartilhamento: `%w`
- Nome de compartilhamento do diretório base nº 2: `%w` - Caminho de compartilhamento: `%d/%w`
- Caminho de pesquisa nº 1: `/vol0home/home`
- Caminho de pesquisa nº 2: `/vol1home/home`
- Caminho de pesquisa nº 3: `/vol2home/home`
- Diretório base: `/vol1home/home/jsmith`

Cenário 1: O usuário se coneta `\\vs1\home_jsmith` ao . Isso corresponde ao primeiro nome de compartilhamento do diretório inicial e gera o caminho `jsmith`relativo . O ONTAP procura agora um diretório nomeado `jsmith` verificando cada caminho de pesquisa em ordem:

- `/vol0home/home/jsmith` não existe; passando para o caminho de pesquisa nº 2.
- `/vol1home/home/jsmith` existe; portanto, o caminho de pesquisa nº 3 não está marcado; o usuário agora está conetado ao seu diretório inicial.

Cenário 2: O usuário se coneta `\\vs1\jsmith` ao . Isso corresponde ao segundo nome de compartilhamento do diretório inicial e gera o caminho `acme/jsmith`relativo . O ONTAP procura agora um diretório nomeado `acme/jsmith` verificando cada caminho de pesquisa em ordem:

- `/vol0home/home/acme/jsmith` não existe; passando para o caminho de pesquisa nº 2.
- `/vol1home/home/acme/jsmith` não existe; passando para o caminho de pesquisa nº 3.
- `/vol2home/home/acme/jsmith` não existe; o diretório home não existe; portanto, a conexão falha.

Compartilhamentos de diretório base

Adicione um compartilhamento de diretório base

Se você quiser usar o recurso diretório base SMB, você deve adicionar pelo menos um compartilhamento com a propriedade diretório base incluída nas propriedades de compartilhamento.

Sobre esta tarefa

Você pode criar um compartilhamento de diretório inicial no momento em que você cria o compartilhamento usando o `vserver cifs share create` comando, ou você pode alterar um compartilhamento existente em um compartilhamento de diretório inicial a qualquer momento usando o `vserver cifs share modify` comando.

Para criar um compartilhamento de diretório inicial, você deve incluir o `homedirectory` valor na `-share -properties` opção quando criar ou modificar um compartilhamento. Você pode especificar o nome do compartilhamento e o caminho do compartilhamento usando variáveis que são expandidas dinamicamente quando os usuários se conetam a seus diretórios base. As variáveis disponíveis que você pode usar no caminho são `%w`, `%d` e `%u`, correspondentes ao nome de usuário, domínio e nome de usuário UNIX mapeado do Windows, respetivamente.

Passos

1. Adicionar um diretório de casa compartilhar
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

   `-share-name` *`share-name`* especifica o nome de compartilhamento do diretório base.

   Além de conter uma das variáveis necessárias, se o nome do compartilhamento contiver uma das strings literais `%w` , `%u`, ou `%d`, você deve preceder a string literal com um caractere % (percentual) para impedir que o ONTAP trate a string literal como uma variável (por exemplo, `%%w`).

   - O nome do compartilhamento deve conter a `%w` variável ou `%u`.
   - O nome do compartilhamento também pode conter a `%d` variável (por exemplo, `%d/%w`) ou uma parte estática no nome do compartilhamento (por exemplo, home1_/`%w`).
   - Se o compartilhamento for usado pelos administradores para se conetar aos diretórios home de outros usuários ou para permitir que os usuários se conetem aos diretórios home de outros usuários, o padrão de nome de compartilhamento dinâmico deve ser precedido por um til (.).

     ```
     `vserver cifs home-directory modify`O é utilizado para ativar este acesso definindo `-is-home-dirs-access-for-admin-enabled` a opção como `true`) ou definindo a opção avançada `-is-home-dirs-access-for-public-enabled` como `true`.
     ```

   `-path path` especifica o caminho relativo para o diretório home.

`-share-properties homedirectory[,…]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

1. Verifique se você adicionou com êxito o compartilhamento do diretório home usando o `vserver cifs share show` comando.

Exemplo

O comando a seguir cria um compartilhamento de diretório base `%w` chamado . As `oplocks` propriedades , `browsable`, e `changenotify` compartilhar são definidas além de definir a `homedirectory` propriedade compartilhar.

> Este exemplo não exibe a saída de todos os compartilhamentos no SVM. A saída é truncada.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Informações relacionadas

Adicionando um caminho de pesquisa de diretório base

Requisitos e diretrizes para o uso de referências automáticas de nós

Gerenciando a acessibilidade aos diretórios home dos usuários

Compartilhamentos de diretório inicial exigem nomes de usuário exclusivos

Tenha cuidado para atribuir nomes de usuário exclusivos ao criar compartilhamentos de diretório inicial usando as `%w` variáveis (nome de usuário do Windows) ou `%u` (nome de usuário UNIX) para gerar compartilhamentos dinamicamente. O nome da partilha é mapeado para o seu nome de utilizador.

Podem ocorrer dois problemas quando o nome de uma partilha estática e o nome de um utilizador são os mesmos:

- Quando o usuário lista os compartilhamentos em um cluster usando o `net view` comando, dois compartilhamentos com o mesmo nome de usuário são exibidos.
- Quando o usuário se coneta a esse nome de compartilhamento, o usuário está sempre conetado ao compartilhamento estático e não pode acessar o compartilhamento do diretório inicial com o mesmo nome.

Por exemplo, há um compartilhamento chamado "administrador" e você tem um nome de usuário do Windows. Se você criar um compartilhamento de diretório base e se conetar a esse compartilhamento, você será conetado ao compartilhamento estático "'administrador'", não ao compartilhamento de diretório principal "'administrador'".

Você pode resolver o problema com nomes de compartilhamento duplicados seguindo qualquer uma destas etapas:

- Renomear o compartilhamento estático para que ele não fique em conflito com o compartilhamento do diretório home do usuário.
- Dando ao usuário um novo nome de usuário para que ele não fique em conflito com o nome de compartilhamento estático.
- Criando um compartilhamento de diretório home CIFS com um nome estático, como "'home'", em vez de

usar o `%w` parâmetro para evitar conflitos com os nomes de compartilhamento.

O que acontece com nomes estáticos de compartilhamento de diretório base após a atualização

Os nomes de compartilhamento de diretório base devem conter a `%w` variável dinâmica ou `%u` . Você deve estar ciente do que acontece com nomes de compartilhamento de diretório home estático existentes após atualizar para uma versão do ONTAP com o novo requisito.

Se a configuração do diretório base contiver nomes de compartilhamento estáticos e você atualizar para o ONTAP, os nomes de compartilhamento do diretório base estático não serão alterados e ainda serão válidos. No entanto, você não pode criar novos compartilhamentos de diretório base que não contenham a `%w` variável ou `%u`.

Exigir que uma dessas variáveis seja incluída no nome de compartilhamento do diretório home do usuário garante que cada nome de compartilhamento seja exclusivo em toda a configuração do diretório home. Se desejar, você pode alterar os nomes estáticos de compartilhamento do diretório base para nomes que contêm a `%w` variável ou `%u`.

Adicione um caminho de pesquisa de diretório base

Se você quiser usar diretórios home do ONTAP SMB, você deve adicionar pelo menos um caminho de pesquisa de diretório base.

Sobre esta tarefa

Você pode adicionar um caminho de pesquisa de diretório base usando o `vserver cifs home-directory search-path add` comando.

O `vserver cifs home-directory search-path add` comando verifica o caminho especificado na `-path` opção durante a execução do comando. Se o caminho especificado não existir, o comando gera uma mensagem solicitando se deseja continuar. Você escolhe `y` ou `n`. Se você optar `y` por continuar, o ONTAP criará o caminho de pesquisa. No entanto, você deve criar a estrutura do diretório antes de usar o caminho de pesquisa na configuração do diretório base. Se você optar por não continuar, o comando falhará; o caminho de pesquisa não será criado. Em seguida, você pode criar a estrutura de diretório de caminho e executar novamente o `vserver cifs home-directory search-path add` comando.

Passos

1. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.

Exemplo

O exemplo a seguir adiciona o caminho `/home1` à configuração do diretório base no SVM VS1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

O exemplo a seguir tenta adicionar o caminho `/home2` à configuração do diretório base no SVM VS1. O caminho não existe. A escolha é feita para não continuar.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informações relacionadas

Adicionando um compartilhamento de diretório inicial

Crie uma configuração de diretório base usando as variáveis %W e %d

Você pode criar uma configuração de diretório base usando as `%w` variáveis e. `%d` Os usuários podem então se conetar ao compartilhamento doméstico usando compartilhamentos criados dinamicamente.

Passos

1. Crie uma qtree para conter os diretórios iniciais do usuário: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verifique se a qtree está usando o estilo de segurança correto: `volume qtree show`
3. Se a qtree não estiver usando o estilo de segurança desejado, altere o estilo de segurança usando o `volume qtree security` comando.
4. Adicionar uma partilha de diretório base: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

   `-share-name %w` especifica o nome de compartilhamento do diretório base. O ONTAP cria dinamicamente o nome do compartilhamento à medida que cada usuário se coneta ao seu diretório inicial. O nome da partilha será do formulário *Windows_user_name*.

   `-path %d/%w` especifica o caminho relativo para o diretório home. O caminho relativo é criado dinamicamente à medida que cada usuário se coneta ao seu diretório inicial e será do formulário *domain/Windows_user_name*.

`-share-properties homedirectory[,…]+` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

5. Verifique se o compartilhamento tem a configuração desejada usando o `vserver cifs share show` comando.
6. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Especifica o SVM habilitado para CIFS no qual adicionar o caminho de pesquisa.

   `-path` *`path`* especifica o caminho absoluto do diretório para o caminho de pesquisa.

7. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.
8. Para usuários com um diretório home, crie um diretório correspondente na qtree ou volume designado para conter diretórios home.

   Por exemplo, se você criou uma qtree com o caminho `/vol/vol1/users` e o nome de usuário cujo diretório você deseja criar é mydomain.user1, você criará um diretório com o seguinte caminho: `/vol/vol1/users/mydomain/user1`.

   Se você criou um volume chamado "'home1" montado no `/home1`, você criará um diretório com o seguinte caminho: `/home1/mydomain/user1`.

9. Verifique se um usuário pode se conetar com êxito ao compartilhamento doméstico mapeando uma unidade ou conetando-se usando o caminho UNC.

   Por exemplo, se o usuário mydomain/user1 quiser se conetar ao diretório criado na Etapa 8 que está localizado na SVM VS1, o user1 se conetaria usando o caminho UNC `\\vs1\user1` .

Exemplo

Os comandos no exemplo a seguir criam uma configuração de diretório base com as seguintes configurações:

- O nome da partilha é %w.
- O caminho do diretório home relativo é %d/%w.
- O caminho de pesquisa usado para conter os diretórios base `/home1` , é um volume configurado com estilo de segurança NTFS.
- A configuração é criada no SVM VS1.

Você pode usar esse tipo de configuração de diretório base quando os usuários acessam seus diretórios base a partir de hosts do Windows. Você também pode usar esse tipo de configuração quando os usuários acessam seus diretórios base a partir de hosts Windows e UNIX e o administrador do sistema de arquivos usa usuários e grupos baseados no Windows para controlar o acesso ao sistema de arquivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                     Vserver: vs1
                       Share: %w
     CIFS Server NetBIOS Name: VS1
                        Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Informações relacionadas

Configurando diretórios base usando a variável %u

Configurações adicionais do diretório base

Exibindo informações sobre o caminho do diretório inicial de um usuário SMB

Configure diretórios base usando a variável %u

Você pode criar uma configuração de diretório inicial onde você designar o nome de compartilhamento usando a `%w` variável, mas você usa a `%u` variável para designar o caminho relativo para o compartilhamento de diretório inicial. Em seguida, os usuários podem se conetar ao compartilhamento doméstico usando compartilhamentos criados dinamicamente usando o nome de usuário do Windows sem estar ciente do nome ou caminho real do diretório inicial.

Passos

1. Crie uma qtree para conter os diretórios iniciais do usuário: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verifique se a qtree está usando o estilo de segurança correto: `volume qtree show`
3. Se a qtree não estiver usando o estilo de segurança desejado, altere o estilo de segurança usando o `volume qtree security` comando.
4. Adicionar uma partilha de diretório base: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

   `-share-name %w` especifica o nome de compartilhamento do diretório base. O nome do compartilhamento é criado dinamicamente à medida que cada usuário se coneta ao seu diretório inicial e é do formulário *Windows_user_name*.

   > Você também pode usar a `%u` variável para a `-share-name` opção. Isso cria um caminho de compartilhamento relativo que usa o nome de usuário UNIX mapeado.

   `-path %u` especifica o caminho relativo para o diretório home. O caminho relativo é criado dinamicamente à medida que cada usuário se coneta ao seu diretório inicial e é do formulário *mapeado_UNIX_user_name*.

   > O valor para esta opção também pode conter elementos estáticos. Por exemplo, `eng/%u`.

   `-share-properties homedirectory\[,...\]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

5. Verifique se o compartilhamento tem a configuração desejada usando o `vserver cifs share show` comando.
6. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Especifica o SVM habilitado para CIFS no qual adicionar o caminho de pesquisa.

   `-path path` especifica o caminho absoluto do diretório para o caminho de pesquisa.

7. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.
8. Se o usuário UNIX não existir, crie o usuário UNIX usando o `vserver services unix-user create` comando.

   > O nome de usuário UNIX para o qual você mapeia o nome de usuário do Windows deve existir antes de mapear o usuário.

9. Crie um mapeamento de nomes para o usuário do Windows para o usuário UNIX usando o seguinte comando: `vserver name-mapping create -vserver vserver_name -direction win-unix`

```
-priority integer -pattern windows_user_name -replacement unix_user_name
```

> Se já existirem mapeamentos de nomes que mapeiem os usuários do Windows para usuários UNIX, você não precisará executar a etapa de mapeamento.

O nome de usuário do Windows é mapeado para o nome de usuário UNIX correspondente. Quando o usuário do Windows se coneta ao compartilhamento do diretório inicial, ele se coneta a um diretório inicial criado dinamicamente com um nome de compartilhamento que corresponde ao nome de usuário do Windows sem saber que o nome do diretório corresponde ao nome de usuário do UNIX.

10. Para usuários com um diretório home, crie um diretório correspondente na qtree ou volume designado para conter diretórios home.

    Por exemplo, se você criou uma qtree com o caminho `/vol/vol1/users` e o nome de usuário UNIX mapeado do usuário cujo diretório você deseja criar é ""unixuser1"", você criará um diretório com o seguinte caminho: `/vol/vol1/users/unixuser1`.

    Se você criou um volume chamado "'home1" montado no `/home1`, você criará um diretório com o seguinte caminho: `/home1/unixuser1`.

11. Verifique se um usuário pode se conetar com êxito ao compartilhamento doméstico mapeando uma unidade ou conetando-se usando o caminho UNC.

    Por exemplo, se o usuário mydomain/user1 mapeia para o usuário UNIX unixuser1 e quiser se conetar ao diretório criado na Etapa 10 que está localizado na SVM VS1, o user1 se conetaria usando o caminho UNC `\\vs1\user1` .

Exemplo

Os comandos no exemplo a seguir criam uma configuração de diretório base com as seguintes configurações:

- O nome da partilha é %w.
- O caminho relativo do diretório base é %u.
- O caminho de pesquisa usado para conter os diretórios base `/home1` , é um volume configurado com estilo de segurança UNIX.
- A configuração é criada no SVM VS1.

Você pode usar esse tipo de configuração de diretório base quando os usuários acessam seus diretórios base de hosts do Windows ou hosts do Windows e UNIX e o administrador do sistema de arquivos usa usuários e grupos baseados em UNIX para controlar o acesso ao sistema de arquivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Informações relacionadas

Criando uma configuração de diretório base usando as variáveis %W e %d

Configurações adicionais do diretório base

Exibindo informações sobre o caminho do diretório inicial de um usuário SMB

Configurações adicionais do diretório base

Você pode criar configurações adicionais do diretório base usando as `%w` variáveis , `%d`, e `%u` , que permitem personalizar a configuração do diretório base para atender às suas necessidades.

Você pode criar uma série de configurações de diretório inicial usando uma combinação de variáveis e strings estáticas nos nomes de compartilhamento e caminhos de pesquisa. A tabela a seguir fornece alguns exemplos ilustrando como criar diferentes configurações de diretório base:

Caminhos criados quando `/vol1/user` **contém diretórios base…**	**Compartilhar comando…**
Para criar um caminho de compartilhamento `\\vs1\~win_username` que direcione o usuário `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Para criar um caminho de compartilhamento `\\vs1\win_username` que direcione o usuário `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Para criar um caminho de compartilhamento `\\vs1\win_username` que direcione o usuário `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Para criar um caminho de compartilhamento `\\vs1\unix_username` que direcione o usuário `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Comandos para gerenciar caminhos de pesquisa

Existem comandos ONTAP específicos para gerenciar caminhos de pesquisa para configurações de diretório base SMB. Por exemplo, existem comandos para adicionar, remover e exibir informações sobre caminhos de pesquisa. Há também um comando para alterar a ordem do caminho de pesquisa.

Se você quiser…	**Use este comando…**
Adicionar um caminho de pesquisa	`vserver cifs home-directory search-path add`
Exibir caminhos de pesquisa	`vserver cifs home-directory search-path show`

Se você quiser…	Use este comando…
Altere a ordem do caminho de pesquisa	`vserver cifs home-directory search-path reorder`
Remova um caminho de pesquisa	`vserver cifs home-directory search-path remove`

Consulte a página de manual de cada comando para obter mais informações.

Exiba informações sobre o caminho do diretório inicial de um usuário SMB

Você pode exibir o caminho do diretório inicial de um usuário SMB na máquina virtual de armazenamento (SVM), que pode ser usado se você tiver vários caminhos de diretório inicial CIFS configurados e quiser ver qual caminho contém o diretório inicial do usuário.

Passo

1. Exiba o caminho do diretório base usando o `vserver cifs home-directory show-user` comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

Informações relacionadas

Gerenciando a acessibilidade aos diretórios home dos usuários

Gerencie a acessibilidade aos diretórios home dos usuários

Por padrão, o diretório home de um usuário só pode ser acessado por esse usuário. Para compartilhamentos em que o nome dinâmico do compartilhamento é precedido por um til ("til"), você pode habilitar ou desabilitar o acesso aos diretórios iniciais dos usuários por administradores do Windows ou por qualquer outro usuário (acesso público).

Antes de começar

Os compartilhamentos de diretório inicial na máquina virtual de armazenamento (SVM) devem ser configurados com nomes de compartilhamento dinâmicos que são precedidos por um til ("tilde"). Os seguintes casos ilustram os requisitos de nomeação de compartilhamento:

Nome de compartilhamento do diretório base	Exemplo de comando para se conetar ao compartilhamento
clique no botão "ok"	`net use * \\IPaddress\~domain~user/u:credentials`

Nome de compartilhamento do diretório base	Exemplo de comando para se conetar ao compartilhamento
clique no botão "ok"	`net use * \\IPaddress\~user/u:credentials`
clique no botão "ok"	`net use * \\IPaddress\abc~user/u:credentials`

Passo

1. Execute a ação apropriada:

Se você quiser ativar ou desativar o acesso aos diretórios home dos usuários para…	Digite o seguinte…
Administradores do Windows	`vserver cifs home-directory modify -vserver` *vserver_name* `-is-home-dirs -access-for-admin-enabled {true|false}` A predefinição é `true`.
Qualquer utilizador (acesso público)	a. Defina o nível de privilégio como avançado `set -privilege advanced` b. Ativar ou desativar o acesso: `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

O exemplo a seguir permite o acesso público aos diretórios home dos usuários

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Informações relacionadas

Exibindo informações sobre o caminho do diretório inicial de um usuário SMB

Configurar o acesso de cliente SMB a links simbólicos UNIX

Como o ONTAP permite que você forneça acesso de cliente SMB a links simbólicos UNIX

Um link simbólico é um arquivo criado em um ambiente UNIX que contém uma referência a outro arquivo ou diretório. Se um cliente acessar um link simbólico, o cliente será redirecionado para o arquivo de destino ou diretório ao qual o link simbólico se refere. O ONTAP suporta links simbólicos relativos e absolutos, incluindo widelinks (links absolutos com alvos fora do sistema de arquivos local).

O ONTAP fornece aos clientes SMB a capacidade de seguir links simbólicos UNIX configurados no SVM. Este recurso é opcional, e você pode configurá-lo por compartilhamento, usando a `-symlink-properties` opção `vserver cifs share create` do comando, com uma das seguintes configurações:

- Habilitado com acesso de leitura/gravação
- Habilitado com acesso somente leitura
- Desabilitado ocultando links simbólicos de clientes SMB
- Desativado sem acesso a links simbólicos de clientes SMB

Se você habilitar links simbólicos em um compartilhamento, links simbólicos relativos funcionam sem configuração adicional.

Se você habilitar links simbólicos em um compartilhamento, links simbólicos absolutos não funcionam imediatamente. Você deve primeiro criar um mapeamento entre o caminho UNIX do link simbólico para o caminho SMB de destino. Ao criar mapeamentos de links simbólicos absolutos, você pode especificar se é um link local ou um *widelink*; widelinks podem ser links para sistemas de arquivos em outros dispositivos de armazenamento ou links para sistemas de arquivos hospedados em SVMs separadas no mesmo sistema ONTAP. Quando você cria um widelink, ele deve incluir as informações para o cliente seguir; ou seja, você cria um ponto de reparação para o cliente descobrir o ponto de junção do diretório. Se você criar um link simbólico absoluto para um arquivo ou diretório fora do compartilhamento local, mas definir a localidade como local, o ONTAP não permite o acesso ao destino.

> Se um cliente tentar excluir um link simbólico local (absoluto ou relativo), apenas o link simbólico é excluído, não o arquivo ou diretório de destino. No entanto, se um cliente tentar excluir um widelink, ele pode excluir o arquivo ou diretório de destino real ao qual o widelink se refere. O ONTAP não tem controle sobre isso porque o cliente pode abrir explicitamente o arquivo ou diretório de destino fora do SVM e excluí-lo.

- **Reparse Points e serviços de sistema de arquivos ONTAP**

  Um *ponto de reparação* é um objeto de sistema de arquivos NTFS que pode ser opcionalmente armazenado em volumes junto com um arquivo. Os pontos Reparse fornecem aos clientes SMB a capacidade de receber serviços de sistema de arquivos aprimorados ou estendidos ao trabalhar com volumes de estilo NTFS. Os pontos Reparse consistem em tags padrão que identificam o tipo de ponto de reparação e o conteúdo do ponto de reparação que pode ser recuperado por clientes SMB para processamento posterior pelo cliente. Dos tipos de objeto disponíveis para a funcionalidade estendida do sistema de arquivos, o ONTAP implementa suporte para links simbólicos NTFS e pontos de junção de diretório usando tags de ponto de reparação. Os clientes SMB que não conseguem entender o conteúdo de um ponto de reparação simplesmente ignoram e não fornecem o serviço de sistema de arquivos estendido que o ponto de reparação pode habilitar.

- * Diretório de pontos de junção e suporte ONTAP para links simbólicos*

  Os pontos de junção de diretório são locais dentro de uma estrutura de diretórios do sistema de arquivos que podem se referir a locais alternativos onde os arquivos são armazenados, seja em um caminho diferente (links simbólicos) ou em um dispositivo de armazenamento separado (widelinks). Os servidores SMB do ONTAP expõem pontos de junção de diretório para clientes Windows como pontos de reparação, permitindo que clientes capazes obtenham conteúdos de pontos de reparação do ONTAP quando um ponto de junção de diretório é atravessado. Eles podem, assim, navegar e se conetar a diferentes caminhos ou dispositivos de armazenamento como se fossem parte do mesmo sistema de arquivos.

- * Habilitando o suporte de widelink usando opções de ponto de reparação*

  A `-is-use-junctions-as-reparse-points-enabled` opção está ativada por predefinição no ONTAP 9. Nem todos os clientes SMB suportam widelinks, portanto, a opção de ativar as informações é configurável com base na versão por protocolo, permitindo que os administradores acomodem clientes SMB com suporte e não suporte. No ONTAP 9.2 e versões posteriores, você deve habilitar a opção

`-widelink-as-reparse-point-versions` para cada protocolo cliente que acessa o compartilhamento usando widelinks; o padrão é SMB1. Em versões anteriores, apenas os widelinks acessados usando o SMB1 padrão foram relatados e os sistemas que usam SMB2 ou SMB3 não conseguiram acessar os widelinks.

Informações relacionadas

- "Aplicativos de backup do Windows e links simbólicos em estilo Unix"
- "Documentação da Microsoft: Pontos de reanálise"

Limites ao configurar links simbólicos UNIX para acesso SMB

Você precisa estar ciente de certos limites ao configurar links simbólicos UNIX para acesso SMB.

Limite	Descrição
45	Comprimento máximo do nome do servidor CIFS que você pode especificar ao usar um FQDN para o nome do servidor CIFS. Você pode, alternativamente, especificar o nome do servidor CIFS como um nome NetBIOS, que é limitado a 15 carateres.
80	Comprimento máximo do nome da partilha.
256	Comprimento máximo do caminho UNIX que você pode especificar ao criar um link simbólico ou ao modificar o caminho UNIX de um link simbólico existente. O caminho UNIX deve começar com um "`"/" (slash) and end with a "/"`". As barras de início e fim contam como parte do limite de 256 carateres.
256	Comprimento máximo do caminho CIFS que você pode especificar ao criar um link simbólico ou ao modificar o caminho CIFS de um link simbólico existente. O caminho CIFS deve começar com um "`"/" (slash) and end with a "/"`". As barras de início e fim contam como parte do limite de 256 carateres.

Informações relacionadas

Criando mapeamentos de links simbólicos para compartilhamentos SMB

Controle anúncios DFS automáticos no ONTAP com uma opção de servidor CIFS

Uma opção de servidor CIFS controla como os recursos do DFS são anunciados para clientes SMB ao se conetar a compartilhamentos. Como o ONTAP usa referências DFS

quando os clientes acessam links simbólicos sobre o SMB, você deve estar ciente do impactos ao desativar ou ativar essa opção.

Uma opção de servidor CIFS determina se os servidores CIFS anunciam automaticamente que são capazes de DFS para clientes SMB. Por padrão, essa opção está ativada e o servidor CIFS sempre anuncia que é capaz de DFS para clientes SMB (mesmo quando se coneta a compartilhamentos onde o acesso a links simbólicos está desativado). Se você quiser que o servidor CIFS anuncie que ele é capaz de clientes somente quando eles estão se conetando a compartilhamentos onde o acesso a links simbólicos está ativado, você pode desativar essa opção.

Você deve estar ciente do que acontece quando essa opção está desativada:

- As configurações de compartilhamento para links simbólicos não são alteradas.
- Se o parâmetro share estiver definido para permitir acesso a links simbólicos (acesso de leitura e gravação ou acesso somente leitura), o servidor CIFS anuncia recursos DFS aos clientes que se conetam a esse compartilhamento.

  As conexões do cliente e o acesso a links simbólicos continuam sem interrupção.

- Se o parâmetro share estiver definido para não permitir acesso a links simbólicos (desabilitando o acesso ou se o valor do parâmetro share for nulo), o servidor CIFS não anunciará recursos DFS aos clientes que se conetam a esse compartilhamento.

  Como os clientes têm informações em cache que o servidor CIFS é capaz de DFS e não está mais anunciando que são, os clientes que estão conetados a compartilhamentos onde o acesso a links simbólicos está desativado podem não ser capazes de acessar esses compartilhamentos depois que a opção do servidor CIFS é desativada. Depois que a opção estiver desativada, talvez seja necessário reinicializar os clientes que estão conetados a esses compartilhamentos, limpando assim as informações em cache.

Essas alterações não se aplicam às conexões SMB 1,0.

Configurar o suporte a links simbólicos UNIX em compartilhamentos SMB

Você pode configurar o suporte a links simbólicos UNIX em compartilhamentos SMB especificando uma configuração de propriedade de compartilhamento de link simbólico ao criar compartilhamentos SMB ou a qualquer momento modificando compartilhamentos SMB existentes. O suporte a links simbólicos UNIX está habilitado por padrão. Você também pode desativar o suporte a links simbólicos UNIX em um compartilhamento.

Sobre esta tarefa

Ao configurar o suporte a links simbólicos UNIX para compartilhamentos SMB, você pode escolher uma das seguintes configurações:

Definição	Descrição
`enable` (OBSOLETO*)	Especifica que links simbólicos estão habilitados para acesso de leitura e gravação.

Definição	Descrição
`read_only` (OBSOLETO*)	Especifica que os links simbólicos estão ativados para acesso somente leitura. Esta definição não se aplica a widelinks. O acesso à Widelink é sempre leitura-escrita.
`hide` (OBSOLETO*)	Especifica que os clientes SMB são impedidos de ver links simbólicos.
`no-strict-security`	Especifica que os clientes seguem links simbólicos fora dos limites de compartilhamento.
`symlinks`	Especifica que os links simbólicos são ativados localmente para acesso de leitura e gravação. Os anúncios DFS não são gerados mesmo que a opção CIFS `is-advertise-dfs-enabled` esteja definida como `true`. Esta é a configuração padrão.
`symlinks-and-widelinks`	Especifica que os links simbólicos locais e os widelinks para acesso de leitura e gravação. Os anúncios DFS são gerados para links simbólicos locais e widelinks, mesmo que a opção CIFS `is-advertise-dfs-enabled` esteja definida como `false`.
`disable`	Especifica que links simbólicos e widelinks estão desativados. Os anúncios DFS não são gerados mesmo que a opção CIFS `is-advertise-dfs-enabled` esteja definida como `true`.
`""` (nulo, não definido)	Desativa links simbólicos no compartilhamento.
– (não definido)	Desativa links simbólicos no compartilhamento.

*Os parâmetros *enable*, *hide* e *read-only* são obsoletos e podem ser removidos em uma versão futura do ONTAP.

Passos

1. Configure ou desative o suporte a links simbólicos:

Se for…	Digite…
Um novo compartilhamento SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only

Se for…	Digite…
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Um compartilhamento SMB existente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Verifique se a configuração do compartilhamento SMB está correta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemplo

O comando a seguir cria um compartilhamento SMB chamado "d.ATA1" com a configuração de link simbólico UNIX definida como `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informações relacionadas

Criando mapeamentos de links simbólicos para compartilhamentos SMB

Crie mapeamentos de links simbólicos para compartilhamentos SMB

Você pode criar mapeamentos de links simbólicos UNIX para compartilhamentos SMB. Você pode criar um link simbólico relativo, que se refere ao arquivo ou pasta relativa à sua pasta pai, ou você pode criar um link simbólico absoluto, que se refere ao arquivo ou pasta usando um caminho absoluto.

Sobre esta tarefa

Os Winelinks não são acessíveis a partir de clientes Mac os X se você usar SMB 2.x. Quando um usuário tenta se conetar a um compartilhamento usando widelinks de um cliente Mac os X, a tentativa falha. No entanto, você pode usar widelinks com clientes Mac os X se você usar SMB 1.

Passos

1. Para criar mapeamentos de links simbólicos para compartilhamentos SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Especifica o nome da máquina virtual de storage (SVM).

   `-unix-path path` Especifica o caminho UNIX. O caminho UNIX deve começar com uma barra (`/`) e deve terminar com uma barra (`/`).

   `-share-name share_name` Especifica o nome do compartilhamento SMB para mapear.

   `-cifs-path path` Especifica o caminho CIFS. O caminho CIFS deve começar com uma barra (`/`) e deve terminar com uma barra (`/`).

   `-cifs-server server_name` Especifica o nome do servidor CIFS. O nome do servidor CIFS pode ser especificado como um nome DNS (por exemplo, mynetwork.cifs.server.com), endereço IP ou nome NetBIOS. O nome NetBIOS pode ser determinado usando o `vserver cifs show` comando. Se este parâmetro opcional não for especificado, o valor padrão será o nome NetBIOS do servidor CIFS local.

   `-locality local|free|widelink`especifica se deseja criar um link local, um link gratuito ou um link simbólico amplo. Um link simbólico local mapeia para o compartilhamento SMB local. Um link simbólico gratuito pode mapear qualquer lugar no servidor SMB local. Um link simbólico amplo mapeia para qualquer compartilhamento SMB na rede. Se não especificar este parâmetro opcional, o valor predefinido é `local.

   `-home-directory true false`especifica se o compartilhamento de destino é um diretório home. Mesmo que esse parâmetro seja opcional, você deve definir esse parâmetro para `true` quando o compartilhamento de destino for configurado como um diretório inicial. A predefinição é `false`.

Exemplo

O comando a seguir cria um mapeamento de link simbólico no SVM chamado VS1. Ele tem o caminho UNIX `/src/` , o nome de compartilhamento SMB "'SOURCE'", o caminho CIFS `/mycompany/source/` e o

endereço IP do servidor CIFS 123.123.123.123, e é um widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Informações relacionadas

Configurando o suporte a links simbólicos UNIX em compartilhamentos SMB

Comandos para gerenciar mapeamentos de links simbólicos

Existem comandos ONTAP específicos para gerenciar mapeamentos de links simbólicos.

Se você quiser…	Use este comando…
Crie um mapeamento de link simbólico	`vserver cifs symlink create`
Exibir informações sobre mapeamentos de links simbólicos	`vserver cifs symlink show`
Modifique um mapeamento de link simbólico	`vserver cifs symlink modify`
Excluir um mapeamento de link simbólico	`vserver cifs symlink delete`

Consulte a página de manual de cada comando para obter mais informações.

Aplicativos de backup do Windows e links simbólicos em estilo Unix

Quando um aplicativo de backup executado no Windows encontra um link simbólico (link simbólico) estilo Unix, o link é seguido e os dados são copiados. Começando com ONTAP 9.15,1, você tem a opção de fazer backup dos links simbólicos em vez dos dados. Esse recurso é totalmente compatível com FlexGroups e FlexVols da ONTAP.

Visão geral

Antes de alterar a forma como o ONTAP lida com links simbólicos durante uma operação de backup do Windows, você deve estar familiarizado com os benefícios, os principais conceitos e as opções de configuração.

Benefícios

Quando esse recurso está desativado ou indisponível, cada link simbólico é percorrido e os dados aos quais ele se vincula são copiados. Por causa disso, dados desnecessários podem às vezes ser copiados e, em certas situações, o aplicativo pode acabar em um loop. Ao invés disso, fazer backup dos links simbólicos evita esses problemas. E como os arquivos de link simbólico são muito pequenos em comparação com os dados na maioria dos casos, os backups levam menos tempo para serem concluídos. O desempenho geral do cluster também pode melhorar devido à redução das operações de e/S.

Ambiente de servidor Windows

Este recurso é compatível com aplicativos de backup executados no Windows. Você deve entender os aspetos técnicos relevantes do ambiente antes de usá-lo.

Atributos estendidos

O Windows suporta atributos estendidos (EA) que formam coletivamente metadados adicionais associados opcionalmente aos arquivos. Esses atributos são usados por vários aplicativos, como o subsistema do Windows para Linux, conforme descrito em "Permissões de arquivo para WSL". Os aplicativos podem solicitar atributos estendidos para cada arquivo ao ler dados do ONTAP.

Os links simbólicos são retornados nos atributos estendidos quando o recurso é ativado. Portanto, um aplicativo de backup deve fornecer suporte padrão EA, que é usado para armazenar os metadados. Alguns utilitários do Windows suportam e preservam os atributos estendidos. No entanto, se o software de backup não suportar backup e restauração dos atributos estendidos, ele não preservará os metadados associados a cada arquivo e não processará os links simbólicos corretamente.

Configuração do Windows

Os aplicativos de backup executados em um servidor Microsoft Windows podem receber um privilégio especial, permitindo que eles ignorem a segurança normal de arquivos. Isso geralmente é feito adicionando os aplicativos ao grupo operadores de backup. Os aplicativos podem então fazer backup e restaurar arquivos conforme necessário, bem como executar outras operações relacionadas ao sistema. Há alterações sutis no protocolo SMB usado pelos aplicativos de backup que podem ser detetadas pelo ONTAP à medida que os dados são lidos e gravados.

Requisitos

O recurso de backup de link simbólico tem vários requisitos, incluindo:

- O cluster está executando o ONTAP 9.15,1 ou posterior.
- Um aplicativo de backup do Windows que recebeu Privileges de backup especial.
- O aplicativo de backup também deve dar suporte a atributos estendidos e solicitá-los durante as operações de backup.
- O recurso de backup de link simbólico do ONTAP está habilitado para o SVM de dados aplicável.

Opções de configuração

Além da CLI do ONTAP, você também pode gerenciar esse recurso usando a API REST. Consulte "Novidades com a API REST e a automação do ONTAP" para obter mais informações. A configuração que determina como o ONTAP processa os links simbólicos em estilo Unix deve ser executada separadamente para cada SVM.

Ative o recurso de backup de link simbólico no ONTAP

Uma opção de configuração foi introduzida a um comando CLI existente com ONTAP 9.15,1. Você pode usar essa opção para ativar ou desativar o processamento de link simbólico estilo Unix.

Antes de começar

Reveja o básico Requisitos. Além disso:

- Ser capaz de elevar seu privilégio CLI para o nível avançado.
- Determine os dados SVM que você deseja modificar. O SVM `vs1` é usado no comando exemplo.

Passos

1. Defina o nível de privilégio avançado.

```
set privilege advanced
```

2. Habilite o backup de arquivos de link simbólico.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Use BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

Use o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma visão geral de filiais

BranchCache foi desenvolvido pela Microsoft para permitir o armazenamento em cache de conteúdo em computadores locais para clientes solicitantes. A implementação do ONTAP do BranchCache pode reduzir a utilização da rede de área ampla (WAN) e fornecer um melhor tempo de resposta de acesso quando os usuários de uma filial acessam conteúdo armazenado em máquinas virtuais de armazenamento (SVMs) usando SMB.

Se você configurar o BranchCache, os clientes do Windows BranchCache primeiro recuperam o conteúdo do SVM e, em seguida, armazenam o conteúdo em um computador dentro da filial. Se outro cliente habilitado para BranchCache na filial solicitar o mesmo conteúdo, o SVM autentica e autoriza o usuário solicitante. Em seguida, o SVM determina se o conteúdo em cache ainda está atualizado e, se estiver, envia os metadados do cliente sobre o conteúdo em cache. O cliente então usa os metadados para recuperar conteúdo diretamente do cache baseado localmente.

Informações relacionadas

Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Requisitos e diretrizes

Suporte à versão BranchCache

Você deve estar ciente de quais versões do BranchCache o ONTAP suporta.

O ONTAP oferece suporte ao BranchCache 1 e ao BranchCache 2 aprimorado:

- Ao configurar o BranchCache no servidor SMB para a máquina virtual de armazenamento (SVM), você pode habilitar o BranchCache 1, o BranchCache 2 ou todas as versões.

  Por padrão, todas as versões estão ativadas.

- Se você ativar apenas o BranchCache 2, as máquinas cliente Windows do escritório remoto devem suportar o BranchCache 2.

  Somente clientes SMB 3,0 ou posteriores suportam BranchCache 2.

Para obter mais informações sobre as versões do BranchCache, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos de suporte ao protocolo de rede

Você deve estar ciente dos requisitos de protocolo de rede para implementar o ONTAP BranchCache.

Você pode implementar o recurso ONTAP BranchCache em redes IPv4 e IPv6 usando SMB 2,1 ou posterior.

Todos os servidores CIFS e máquinas de filiais que participam da implementação do BranchCache devem ter o protocolo SMB 2,1 ou posterior ativado. O SMB 2,1 tem extensões de protocolo que permitem que um cliente participe de um ambiente BranchCache. Esta é a versão mínima do protocolo SMB que oferece suporte ao BranchCache. O SMB 2,1 suporta a versão BranchCache 1.

Se você quiser usar o BranchCache versão 2, o SMB 3,0 é a versão mínima suportada. Todos os servidores CIFS e máquinas de filiais que participam de uma implementação BranchCache 2 devem ter o SMB 3,0 ou posterior habilitado.

Se você tiver escritórios remotos onde alguns dos clientes suportam apenas o SMB 2,1 e alguns dos clientes suportam o SMB 3,0, você pode implementar uma configuração BranchCache no servidor CIFS que fornece suporte de cache tanto no BranchCache 1 quanto no BranchCache 2.

Embora o recurso Microsoft BranchCache suporte ao uso dos protocolos HTTP/HTTPS e SMB como protocolos de acesso a arquivos, o ONTAP BranchCache só suporta o uso de SMB.

O ONTAP e o Windows hosts requisitos de versão

Os hosts do ONTAP e da filial do Windows devem atender a certos requisitos de versão antes de poder configurar o BranchCache.

Antes de configurar o BranchCache, você deve garantir que a versão do ONTAP no cluster e clientes de filiais participantes ofereçam suporte ao SMB 2,1 ou posterior e ofereça suporte ao recurso BranchCache. Se você configurar o modo Cache hospedado, você também deve garantir que você use um host suportado para o servidor de cache.

O BranchCache 1 é compatível com as seguintes versões do ONTAP e hosts do Windows:

- Servidor de conteúdo: Máquina virtual de storage (SVM) com ONTAP
- Servidor de cache: Windows Server 2008 R2 ou Windows Server 2012 ou posterior
- Peer ou cliente: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 ou posterior

O BranchCache 2 é compatível com as seguintes versões do ONTAP e hosts do Windows:

- Servidor de conteúdo: SVM com ONTAP
- Servidor de cache: Windows Server 2012 ou posterior
- Peer ou cliente: Windows 8 ou Windows Server 2012 ou posterior

Razões pelas quais o ONTAP invalida hashes do BranchCache

Entender as razões pelas quais o ONTAP invalida hashes pode ser útil ao Planejar sua configuração do BranchCache. Ele pode ajudá-lo a decidir qual modo de operação você deve configurar e pode ajudá-lo a escolher em quais compartilhamentos ativar o BranchCache.

O ONTAP deve gerenciar hashes do BranchCache para garantir que os hashes sejam válidos. Se um hash não for válido, o ONTAP invalida o hash e computa um novo hash na próxima vez que o conteúdo for solicitado, supondo que o BranchCache ainda esteja habilitado.

O ONTAP invalida hashes pelos seguintes motivos:

- A chave do servidor é modificada.

  Se a chave do servidor for modificada, o ONTAP invalida todos os hashes no armazenamento de hash.

- Um hash é removido do cache porque o tamanho máximo do armazenamento de hash BranchCache foi atingido.

  Este é um parâmetro sintonizável e pode ser modificado para atender aos requisitos da sua empresa.

- Um arquivo é modificado por meio do acesso SMB ou NFS.
- Um arquivo para o qual há hashes computados é restaurado usando o `snap restore` comando.
- Um volume que contém compartilhamentos SMB habilitados para BranchCache é restaurado usando o `snap restore` comando.

Diretrizes para escolher o local de armazenamento de hash

Ao configurar o BranchCache, você escolhe onde armazenar hashes e qual tamanho o armazenamento de hash deve ser. Entender as diretrizes ao escolher o local e o tamanho do armazenamento de hash pode ajudá-lo a Planejar sua configuração do BranchCache em um SVM habilitado para CIFS.

- Você deve localizar o armazenamento de hash em um volume onde atualizações de tempo são permitidas.

  O tempo de acesso em um arquivo hash é usado para manter os arquivos acessados com frequência no armazenamento de hash. Se as atualizações do atime estiverem desativadas, a hora de criação será usada para esse fim. É preferível usar o tempo para rastrear arquivos usados com frequência.

- Não é possível armazenar hashes em sistemas de arquivos somente leitura, como destinos SnapMirror e volumes SnapLock.
- Se o tamanho máximo do armazenamento de hash for atingido, os hashes mais antigos serão lavados para abrir espaço para novos hashes.

  Você pode aumentar o tamanho máximo do armazenamento de hash para reduzir a quantidade de hashes que são lavados do cache.

- Se o volume no qual você armazena hashes estiver indisponível ou cheio, ou se houver um problema com a comunicação intra-cluster em que o serviço BranchCache não pode recuperar informações de hash, os serviços BranchCache não estarão disponíveis.

O volume pode estar indisponível porque está offline ou porque o administrador de armazenamento especificou um novo local para o armazenamento de hash.

Isso não causa problemas com acesso a arquivos. Se o acesso ao armazenamento de hash for impedido, o ONTAP retornará um erro definido pela Microsoft ao cliente, o que faz com que o cliente solicite o arquivo usando a solicitação de leitura normal de SMB.

Informações relacionadas

Configure o BranchCache no servidor SMB

Modifique a configuração do BranchCache

Recomendações do BranchCache

Antes de configurar o BranchCache, há certas recomendações que você deve ter em mente ao decidir quais compartilhamentos SMB você deseja ativar o armazenamento em cache do BranchCache.

Você deve ter em mente as seguintes recomendações ao decidir em qual modo de operação usar e em quais compartilhamentos SMB para ativar o BranchCache:

- Os benefícios do BranchCache são reduzidos quando os dados a serem armazenados remotamente em cache são alterados com frequência.
- Os serviços BranchCache são benéficos para compartilhamentos que contêm conteúdo de arquivo que é reutilizado por vários clientes de escritório remoto ou por conteúdo de arquivo que é repetidamente acessado por um único usuário remoto.
- Considere ativar o armazenamento em cache para conteúdo somente leitura, como dados em cópias Snapshot e destinos SnapMirror.

Configurar BranchCache

Configurar visão geral do BranchCache

Você configura o BranchCache no servidor SMB usando comandos ONTAP. Para implementar o BranchCache, você também deve configurar seus clientes e, opcionalmente, seus servidores de cache hospedados nas filiais onde você deseja armazenar conteúdo em cache.

Se você configurar o BranchCache para habilitar o armazenamento em cache de forma compartilhada, você deverá habilitar o BranchCache nos compartilhamentos SMB para os quais deseja fornecer serviços de armazenamento em cache do BranchCache.

Requisitos para configurar o BranchCache

Depois de atender a alguns pré-requisitos, você pode configurar o BranchCache.

Antes de configurar o BranchCache no servidor CIFS para sua SVM, você precisa atender aos requisitos a seguir:

- O ONTAP deve ser instalado em todos os nós do cluster.
- O CIFS deve ser licenciado e um servidor SMB deve ser configurado. A licença SMB está incluída no

"ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

- A conetividade de rede IPv4G ou IPv6G deve ser configurada.
- Para BranchCache 1, o SMB 2,1 ou posterior deve estar ativado.
- Para BranchCache 2, o SMB 3,0 deve estar ativado e os clientes remotos do Windows devem suportar o BranchCache 2.

Configure o BranchCache no servidor SMB

Você pode configurar o BranchCache para fornecer serviços do BranchCache por compartilhamento. Como alternativa, você pode configurar o BranchCache para ativar automaticamente o cache em todos os compartilhamentos SMB.

Sobre esta tarefa

Você pode configurar o BranchCache em SVMs.

- Você pode criar uma configuração BranchCache de todos os compartilhamentos se quiser oferecer serviços de cache para todo o conteúdo contido em todos os compartilhamentos SMB no servidor CIFS.
- Você pode criar uma configuração de BranchCache por compartilhamento se quiser oferecer serviços de cache para conteúdo contido em compartilhamentos SMB selecionados no servidor CIFS.

Você deve especificar os seguintes parâmetros ao configurar o BranchCache:

Parâmetros necessários	Descrição
Nome da SVM	O BranchCache é configurado por SVM. Você deve especificar em qual SVM habilitado para CIFS deseja configurar o serviço BranchCache.
Path to hash store	Os hashes do BranchCache são armazenados em arquivos regulares no volume SVM. Você deve especificar o caminho para um diretório existente onde você deseja que o ONTAP armazene os dados de hash.o caminho de hash do BranchCache deve ser lido-gravável. Caminhos somente leitura, como diretórios Snapshot, não são permitidos. Você pode armazenar dados de hash em um volume que contém outros dados ou pode criar um volume separado para armazenar dados de hash. Se o SVM for uma fonte de recuperação de desastres SVM, o caminho hash não poderá estar no volume raiz. Isso ocorre porque o volume raiz não é replicado para o destino de recuperação de desastres. O caminho hash pode conter espaços em branco e quaisquer carateres de nome de arquivo válidos.

Opcionalmente, você pode especificar os seguintes parâmetros:

Parâmetros opcionais	Descrição
Versões suportadas	ONTAP suporta BranchCache 1 e 2. Pode ativar a versão 1, a versão 2 ou ambas as versões. O padrão é ativar ambas as versões.
Tamanho máximo do armazenamento de hash	Você pode especificar o tamanho a ser usado para o armazenamento de dados de hash. Se os dados de hash excederem esse valor, o ONTAP excluirá hashes mais antigos para abrir espaço para hashes mais recentes. O tamanho padrão para o armazenamento de hash é de 1 GB. O BranchCache funciona de forma mais eficiente se os hashes não forem descartados de forma excessivamente agressiva. Se você determinar que hashes são descartados frequentemente porque o armazenamento de hash está cheio, você pode aumentar o tamanho do armazenamento de hash modificando a configuração BranchCache.
Chave do servidor	Você pode especificar uma chave de servidor que o serviço BranchCache usa para impedir que os clientes personificem o servidor BranchCache. Se você não especificar uma chave de servidor, uma será gerada aleatoriamente quando você criar a configuração BranchCache. Você pode definir a chave do servidor para um valor específico para que, se vários servidores estiverem fornecendo dados do BranchCache para os mesmos arquivos, os clientes possam usar hashes de qualquer servidor usando essa mesma chave do servidor. Se a chave do servidor contiver espaços, você deverá inserir a chave do servidor entre aspas.
Modo de funcionamento	O padrão é habilitar o BranchCache por compartilhamento. • Para criar uma configuração do BranchCache na qual você habilite o BranchCache por compartilhamento, não é possível especificar esse parâmetro opcional ou especificar `per-share`. • Para ativar automaticamente o BranchCache em todos os compartilhamentos, você deve definir o modo operacional como `all-shares`.

Passos

1. Habilite o SMB 2,1 e 3,0 conforme necessário:
   a. Defina o nível de privilégio como avançado: `set -privilege advanced`
   b. Verifique as configurações configuradas do SVM SMB para determinar se todas as versões

necessárias do SMB estão ativadas: `vserver cifs options show -vserver vserver_name`

c. Se necessário, ative o SMB 2,1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

   O comando habilita o SMB 2,0 e o SMB 2,1.

d. Se necessário, ative o SMB 3,0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

e. Voltar ao nível de privilégio de administrador: `set -privilege admin`

2. Configurar BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   O caminho de storage de hash especificado deve existir e residir em um volume gerenciado pela SVM. O caminho também deve estar localizado em um volume gravável de leitura. O comando falha se o caminho for somente leitura ou não existir.

   Se você quiser usar a mesma chave de servidor para configurações adicionais do SVM BranchCache, Registre o valor inserido para a chave de servidor. A chave do servidor não aparece quando você exibe informações sobre a configuração do BranchCache.

3. Verifique se a configuração do BranchCache está correta: `vserver cifs branchcache show -vserver vserver_name`

Exemplos

Os comandos a seguir verificam se o SMB 2,1 e o 3,0 estão ativados e configuram o BranchCache para habilitar automaticamente o armazenamento em cache em todos os compartilhamentos SMB no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Os comandos a seguir verificam se o SMB 2,1 e o 3,0 estão ativados, configuram o BranchCache para habilitar o armazenamento em cache por compartilhamento no SVM VS1 e verificam a configuração do BranchCache:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informações relacionadas

Requisitos e diretrizes: Suporte à versão BranchCache

Onde encontrar informações sobre como configurar o BranchCache no escritório remoto

Crie um compartilhamento SMB habilitado para BranchCache

Ative o BranchCache em um compartilhamento SMB existente

Modifique a configuração do BranchCache

Desative a visão geral de BranchCache na SMB shares

Exclua a configuração BranchCache em SVMs

Onde encontrar informações sobre como configurar o BranchCache no escritório remoto

Depois de configurar o BranchCache no servidor SMB, você deve instalar e configurar o BranchCache em computadores clientes e, opcionalmente, em servidores de cache em seu escritório remoto. A Microsoft fornece instruções para configurar o BranchCache no escritório remoto.

Instruções para configurar clientes de filiais e, opcionalmente, colocar em cache servidores para usar o BranchCache estão no site do Microsoft BranchCache.

"Microsoft BranchCache Docs: O que há de novo"

Configurar compartilhamentos SMB habilitados para BranchCache

Configure a visão geral de compartilhamentos SMB habilitados para BranchCache

Depois de configurar o BranchCache no servidor SMB e na filial, você pode habilitar o BranchCache em compartilhamentos SMB que contenham conteúdo que você deseja permitir que os clientes nas filiais armazenem cache.

O cache BranchCache pode ser ativado em todos os compartilhamentos SMB no servidor SMB ou em uma base de compartilhamento por compartilhamento.

- Se você ativar o BranchCache de forma compartilhada, poderá ativar o BranchCache à medida que você cria o compartilhamento ou modificando compartilhamentos existentes.

  Se você habilitar o armazenamento em cache em um compartilhamento SMB existente, o ONTAP começará a computar hashes e enviar metadados para clientes solicitando conteúdo assim que você ativar o BranchCache nesse compartilhamento.

- Quaisquer clientes que tenham uma conexão SMB existente a um compartilhamento não recebem suporte do BranchCache se o BranchCache for posteriormente habilitado nesse compartilhamento.

  O ONTAP anuncia o suporte do BranchCache para um compartilhamento no momento em que a sessão SMB é configurada. Os clientes que já tiverem sessões estabelecidas quando o BranchCache estiver habilitado precisam se desconetar e se reconetar para usar o conteúdo em cache para esse compartilhamento.

> Se o BranchCache em um compartilhamento SMB for posteriormente desativado, o ONTAP interrompe o envio de metadados para o cliente solicitante. Um cliente que precisa de dados recupera-os diretamente do servidor de conteúdo (servidor SMB).

Crie um compartilhamento SMB habilitado para BranchCache

Você pode ativar o BranchCache em um compartilhamento SMB ao criar o compartilhamento definindo a `branchcache` propriedade compartilhar.

Sobre esta tarefa

- Se o BranchCache estiver ativado no compartilhamento SMB, o compartilhamento deve ter a configuração de arquivos off-line definida como cache manual.

  Esta é a configuração padrão quando você cria um compartilhamento.

- Você também pode especificar parâmetros opcionais adicionais de compartilhamento quando você cria o compartilhamento habilitado para BranchCache.
- Você pode definir a `branchcache` propriedade em um compartilhamento, mesmo que o BranchCache não esteja configurado e habilitado na máquina virtual de storage (SVM).

  No entanto, se você quiser que o compartilhamento ofereça conteúdo em cache, configure e ative o

BranchCache no SVM.

- Como não há propriedades de compartilhamento padrão aplicadas ao compartilhamento quando você usa o `-share-properties` parâmetro, você deve especificar todas as outras propriedades de compartilhamento que deseja aplicar ao compartilhamento além da `branchcache` propriedade de compartilhamento usando uma lista delimitada por vírgulas.
- Para obter mais informações, consulte a página man para o `vserver cifs share create` comando.

Passo

1. Crie um compartilhamento SMB habilitado para BranchCache
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Verifique se a propriedade BranchCache Share está definida no compartilhamento SMB usando o `vserver cifs share show` comando.

Exemplo

O comando a seguir cria um compartilhamento SMB habilitado para BranchCache chamado "data" com um caminho de `/data` no SVM VS1. Por padrão, a configuração arquivos off-line é definida como `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
              Share Properties: branchcache
                                oplocks
                                browsable
                                changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                 Offline Files: manual
Vscan File-Operations Profile: standard
```

Informações relacionadas

Desativar BranchCache em um único compartilhamento SMB

Ative o BranchCache em um compartilhamento SMB existente

Você pode ativar o BranchCache em um compartilhamento SMB existente adicionando a

`branchcache` propriedade share à lista existente de propriedades de compartilhamento.

Sobre esta tarefa

- Se o BranchCache estiver ativado no compartilhamento SMB, o compartilhamento deve ter a configuração de arquivos off-line definida como cache manual.

  Se a configuração arquivos offline do compartilhamento existente não estiver definida como armazenamento manual em cache, você deverá configurá-lo modificando o compartilhamento.

- Você pode definir a `branchcache` propriedade em um compartilhamento, mesmo que o BranchCache não esteja configurado e habilitado na máquina virtual de storage (SVM).

  No entanto, se você quiser que o compartilhamento ofereça conteúdo em cache, configure e ative o BranchCache no SVM.

- Quando você adiciona a `branchcache` propriedade de compartilhamento ao compartilhamento, as configurações de compartilhamento existentes e as propriedades de compartilhamento são preservadas.

  A propriedade de compartilhamento BranchCache é adicionada à lista existente de propriedades de compartilhamento. Para obter mais informações sobre como usar o `vserver cifs share properties add` comando, consulte as páginas de manual.

Passos

1. Se necessário, configure a configuração de compartilhamento de arquivos offline para cache manual:
   a. Determine qual é a configuração de compartilhamento de arquivos off-line usando o `vserver cifs share show` comando.
   b. Se a definição de partilha de ficheiros offline não estiver definida para manual, altere-a para o valor pretendido: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Ativar BranchCache em um compartilhamento SMB existente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verifique se a propriedade BranchCache Share está definida no compartilhamento SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemplo

O comando a seguir habilita o BranchCache em um compartilhamento SMB existente chamado "ata2" com um caminho `/data2` de no SVM VS1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informações relacionadas

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Desativar BranchCache em um único compartilhamento SMB

Gerencie e monitore a configuração do BranchCache

Modifique as configurações do BranchCache

Você pode modificar a configuração do serviço BranchCache em SVMs, incluindo alterar o caminho do diretório de armazenamento de hash, o tamanho máximo do diretório de armazenamento de hash, o modo operacional e quais versões do BranchCache são suportadas. Você também pode aumentar o tamanho do volume que contém o armazenamento de hash.

Passos

1. Execute a ação apropriada:

Se você quiser…	Digite o seguinte…
Modifique o tamanho do diretório de armazenamento de hash	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Aumente o tamanho do volume que contém o armazenamento de hash	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Se o volume que contém o armazenamento de hash for preenchido, você poderá aumentar o tamanho do volume. Você pode especificar o novo tamanho de volume como um número seguido de uma designação de unidade. Saiba mais sobre "Gerenciamento de volumes do FlexVol"	Modifique o caminho do diretório de armazenamento de hash

Se você quiser…	Digite o seguinte…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Se o SVM for uma fonte de recuperação de desastres SVM, o caminho hash não poderá estar no volume raiz. Isso ocorre porque o volume raiz não é replicado para o destino de recuperação de desastres. O caminho hash BranchCache pode conter espaços em branco e quaisquer carateres de nome de arquivo válidos. Se você modificar o caminho de hash, `-flush -hashes` é um parâmetro obrigatório que especifica se você deseja que o ONTAP lave os hashes do local de armazenamento de hash original. Pode definir os seguintes valores para o `-flush -hashes` parâmetro: **Se você especificar `true`, o ONTAP excluirá os hashes no local original e criará novos hashes no novo local à medida que novas solicitações forem feitas por clientes habilitados para BranchCache.** Se você especificar `false`, os hashes não serão lavados. + Nesse caso, você pode optar por reutilizar os hashes existentes mais tarde alterando o caminho de armazenamento de hash de volta para o local original.
Altere o modo de funcionamento	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Ao modificar o modo de funcionamento, deve estar ciente do seguinte: **O ONTAP anuncia o suporte do BranchCache para um compartilhamento quando a sessão SMB está configurada.** Os clientes que já tiverem sessões estabelecidas quando o BranchCache estiver habilitado precisam se desconetar e se reconetar para usar o conteúdo em cache para esse compartilhamento.
Altere o suporte à versão do BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Verifique as alterações de configuração usando o `vserver cifs branchcache show` comando.

Exibir informações sobre configurações do BranchCache

Você pode exibir informações sobre as configurações do BranchCache em máquinas virtuais de armazenamento (SVMs), que podem ser usadas ao verificar uma configuração ou ao determinar as configurações atuais antes de modificar uma configuração.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir…	Digite este comando…
Informações resumidas sobre as configurações do BranchCache em todos os SVMs	`vserver cifs branchcache show`
Informações detalhadas sobre a configuração em uma SVM específica	`vserver cifs branchcache show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe informações sobre a configuração BranchCache no SVM VS1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
           Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Altere a chave do servidor BranchCache

Você pode alterar a chave do servidor BranchCache modificando a configuração BranchCache na máquina virtual de armazenamento (SVM) e especificando uma chave de servidor diferente.

Sobre esta tarefa

Você pode definir a chave do servidor para um valor específico para que, se vários servidores estiverem fornecendo dados do BranchCache para os mesmos arquivos, os clientes possam usar hashes de qualquer servidor usando essa mesma chave do servidor.

Quando você altera a chave do servidor, você também deve lavar o cache hash. Depois de limpar os hashes, o ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Passos

1. Altere a chave do servidor usando o seguinte comando: `vserver cifs branchcache modify`

`-vserver vserver_name -server-key text -flush-hashes true`

Ao configurar uma nova chave de servidor, você também deve especificar `-flush-hashes` e definir o valor como `true`.

2. Verifique se a configuração BranchCache está correta usando o `vserver cifs branchcache show` comando.

Exemplo

O exemplo a seguir define uma nova chave de servidor que contém espaços e limpa o cache de hash no SVM VS1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informações relacionadas

Razões pelas quais o ONTAP invalida hashes do BranchCache

O BranchCache pré-computar hashes em caminhos especificados

Você pode configurar o serviço BranchCache para pré-calcular hashes para um único arquivo, para um diretório ou para todos os arquivos em uma estrutura de diretório. Isso pode ser útil se você quiser calcular hashes de dados em um compartilhamento habilitado pelo BranchCache durante horas fora do horário de pico.

Sobre esta tarefa

Se você quiser coletar uma amostra de dados antes de exibir estatísticas de hash, você deve usar os `statistics start` comandos e opcionais `statistics stop`.

- É necessário especificar a máquina virtual de storage (SVM) e o caminho no qual você deseja pré-calcular hashes.
- Você também deve especificar se deseja que os hashes sejam computados recursivamente.
- Se você quiser que os hashes sejam computados recursivamente, o serviço BranchCache percorre toda a árvore de diretórios sob o caminho especificado e calcula hashes para cada objeto elegível.

Passos

1. Pré-calcular hashes como desejado:

Se você quiser pré-calcular hashes em…	Digite o comando…
Um único arquivo ou diretório	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Recursivamente em todos os arquivos em uma estrutura de diretório	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verifique se os hashes estão sendo computados usando o `statistics` comando:
   a. Exiba estatísticas para o `hashd` objeto na instância SVM desejada: `statistics show -object hashd -instance vserver_name`
   b. Verifique se o número de hashes criados está aumentando repetindo o comando.

Exemplos

O exemplo a seguir cria hashes no caminho `/data` e em todos os arquivos e subdiretórios contidos no SVM VS1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Lave os hashes do armazenamento de hash do SVM BranchCache

Você pode lavar todos os hashes armazenados em cache do armazenamento de hash BranchCache na máquina virtual de armazenamento (SVM). Isso pode ser útil se você tiver alterado a configuração BranchCache da filial. Por exemplo, se você reconfigurou recentemente o modo de armazenamento em cache de armazenamento distribuído para o modo de armazenamento em cache hospedado, você deseja limpar o armazenamento de hash.

Sobre esta tarefa

Depois de limpar os hashes, o ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Passo

1. Lave os hashes do armazenamento de hash BranchCache: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Exibir estatísticas do BranchCache

Você pode exibir estatísticas do BranchCache para, entre outras coisas, identificar o desempenho do cache, determinar se sua configuração está fornecendo conteúdo em cache para clientes e determinar se os arquivos hash foram excluídos para dar espaço aos dados de hash mais recentes.

Sobre esta tarefa

O `hashd` objeto estatístico contém contadores que fornecem informações estatísticas sobre hashes BranchCache. O `cifs` objeto estatístico contém contadores que fornecem informações estatísticas sobre a atividade relacionada ao BranchCache. Você pode coletar e exibir informações sobre esses objetos no nível avançado de privilégios.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Exiba os contadores relacionados ao BranchCache usando o `statistics catalog counter show` comando.

   Para obter mais informações sobre contadores de estatísticas, consulte a página de manual deste comando.

   ```
   ```

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    --------------------------
-------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
```

```
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
    ....Output truncated....
```

3. Colete estatísticas relacionadas ao BranchCache usando os `statistics start` comandos e. `statistics stop`

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. Exiba as estatísticas coletadas do BranchCache usando o `statistics show` comando.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

5. Voltar ao nível de privilégio de administrador: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Informações relacionadas

Exibindo estatísticas

"Configuração do monitoramento de desempenho"

Suporte para objetos de Diretiva de Grupo BranchCache

O ONTAP BranchCache fornece suporte para objetos de Diretiva de Grupo (GPOs) do

BranchCache, que permitem o gerenciamento centralizado para determinados parâmetros de configuração do BranchCache. Existem dois GPOs usados para BranchCache, a publicação Hash para BranchCache GPO e o suporte de versão Hash para BranchCache GPO.

- **Publicação Hash para o GPO BranchCache**

  A publicação Hash para BranchCache GPO corresponde ao `-operating-mode` parâmetro. Quando ocorrem atualizações de GPO, esse valor é aplicado a objetos de máquina virtual de armazenamento (SVM) contidos na unidade organizacional (ou) à qual a diretiva de grupo se aplica.

- **Suporte a versão Hash para o GPO BranchCache**

  O suporte de versão Hash para GPO BranchCache corresponde ao `-versions` parâmetro. Quando ocorrem atualizações de GPO, esse valor é aplicado a objetos SVM contidos na unidade organizacional à qual a diretiva de grupo se aplica.

Informações relacionadas

Aplicando objetos de Diretiva de Grupo a servidores CIFS

Exibir informações sobre os objetos de Diretiva de Grupo BranchCache

Você pode exibir informações sobre a configuração GPO (Group Policy Object) do servidor CIFS para determinar se os GPOs de BranchCache estão definidos para o domínio ao qual o servidor CIFS pertence e, em caso afirmativo, quais são as configurações permitidas. Você também pode determinar se as configurações de GPO do BranchCache são aplicadas ao servidor CIFS.

Sobre esta tarefa

Embora uma configuração de GPO seja definida dentro do domínio ao qual o servidor CIFS pertence, ela não é necessariamente aplicada à unidade organizacional (ou) que contém a máquina virtual de armazenamento (SVM) habilitada para CIFS. A configuração de GPO aplicada é o subconjunto de todos os GPOs definidos que são aplicados ao SVM habilitado para CIFS. As configurações do BranchCache aplicadas por meio de GPOs substituem as configurações aplicadas por meio da CLI.

Passos

1. Exiba a configuração de GPO BranchCache definida para o domínio do ative Directory usando o `vserver cifs group-policy show-defined` comando.

   Este exemplo não exibe todos os campos de saída disponíveis para o comando. A saída é truncada.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Exiba a configuração de GPO BranchCache aplicada ao servidor CIFS usando o `vserver cifs group-policy show-applied` comando. ""

> Este exemplo não exibe todos os campos de saída disponíveis para o comando. A saída é truncada.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Desativar BranchCache em compartilhamentos SMB

Desative a visão geral de BranchCache na SMB shares

Se você não quiser fornecer serviços de armazenamento em cache BranchCache em determinados compartilhamentos SMB, mas talvez queira fornecer serviços de armazenamento em cache nesses compartilhamentos posteriormente, você pode desativar o BranchCache de forma compartilhada. Se você tiver o BranchCache configurado para oferecer armazenamento em cache em todos os compartilhamentos, mas quiser desativar temporariamente todos os serviços de armazenamento em cache, você pode modificar a configuração do BranchCache para interromper o armazenamento em cache automático em todos os compartilhamentos.

Se o BranchCache em um compartilhamento SMB for posteriormente desativado após a primeira ativação, o ONTAP pára de enviar metadados para o cliente solicitante. Um cliente que precisa de dados os recupera diretamente do servidor de conteúdo (servidor CIFS na máquina virtual de armazenamento (SVM)).

Informações relacionadas

Configurando compartilhamentos SMB habilitados para BranchCache

Desative o BranchCache em um único compartilhamento SMB

Se você não quiser oferecer serviços de armazenamento em cache em determinados compartilhamentos que ofereciam conteúdo em cache anteriormente, você pode desativar o BranchCache em um compartilhamento SMB existente.

Passo

1. Introduza o seguinte comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   A propriedade BranchCache Share foi removida. Outras propriedades de compartilhamento aplicadas permanecem em vigor.

Exemplo

O comando a seguir desativa o BranchCache em um compartilhamento SMB existente chamado "ata2":

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Parar o armazenamento em cache automático em todos os compartilhamentos SMB

Se a configuração do BranchCache ativar automaticamente o armazenamento em cache em todos os compartilhamentos SMB em cada máquina virtual de storage (SVM), você poderá modificar a configuração do BranchCache para interromper o armazenamento em cache automático de conteúdo para todos os compartilhamentos SMB.

Sobre esta tarefa

Para interromper o armazenamento em cache automático em todos os compartilhamentos SMB, você altera o modo operacional BranchCache para cache por compartilhamento.

Passos

1. Configure o BranchCache para interromper o armazenamento em cache automático em todos os compartilhamentos SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verifique se a configuração do BranchCache está correta: `vserver cifs branchcache show -vserver vserver_name`

Exemplo

O comando a seguir altera a configuração BranchCache na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1 para parar o armazenamento em cache automático em todos os compartilhamentos SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Desative ou ative o BranchCache no SVM

O que acontece quando você desativa ou rehabilita o BranchCache no servidor CIFS

Se você configurou anteriormente o BranchCache, mas não quer que os clientes da filial usem conteúdo em cache, você pode desativar o cache no servidor CIFS. Você deve estar ciente do que acontece quando você desativa o BranchCache.

Quando você desativa o BranchCache, o ONTAP não computa hashes ou envia os metadados para o cliente solicitante. No entanto, não há interrupção no acesso aos arquivos. Depois disso, quando clientes habilitados para BranchCache solicitam informações de metadados para conteúdo que desejam acessar, o ONTAP responde com um erro definido pela Microsoft, que faz com que o cliente envie uma segunda solicitação, solicitando o conteúdo real. Em resposta à solicitação de conteúdo, o servidor CIFS envia o conteúdo real

armazenado na máquina virtual de storage (SVM).

Depois que o BranchCache é desativado no servidor CIFS, os compartilhamentos SMB não anunciam os recursos do BranchCache. Para acessar dados em novas conexões SMB, os clientes fazem solicitações normais de leitura SMB.

Você pode reativar o BranchCache no servidor CIFS a qualquer momento.

- Como o armazenamento de hash não é excluído quando você desabilita o BranchCache, o ONTAP pode usar os hashes armazenados ao responder a solicitações de hash depois de reativar o BranchCache, desde que o hash solicitado ainda seja válido.
- Quaisquer clientes que tenham feito conexões SMB com compartilhamentos habilitados para BranchCache durante o tempo em que o BranchCache foi desativado não recebem suporte para BranchCache se o BranchCache for posteriormente reativado.

  Isso ocorre porque o ONTAP anuncia o suporte do BranchCache para um compartilhamento no momento em que a sessão SMB é configurada. Os clientes que estabeleceram sessões para compartilhamentos habilitados para BranchCache enquanto o BranchCache foi desativado precisam se desconetar e se reconetar para usar conteúdo em cache para esse compartilhamento.

> Se você não quiser salvar o armazenamento de hash depois de desativar o BranchCache em um servidor CIFS, você pode excluí-lo manualmente. Se você rehabilitar o BranchCache, você deve garantir que o diretório de armazenamento de hash existe. Depois que o BranchCache é reativado, os compartilhamentos habilitados para BranchCache anunciam os recursos do BranchCache. O ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Desative ou ative o BranchCache

Você pode desativar o BranchCache na máquina virtual de armazenamento (SVM) alterando o modo operacional BranchCache para `disabled`. Você pode ativar o BranchCache a qualquer momento alterando o modo operacional para oferecer serviços BranchCache por compartilhamento ou automaticamente para todos os compartilhamentos.

Passos

1. Execute o comando apropriado:

Se você quiser…	Em seguida, digite o seguinte…
Desativar BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Ativar BranchCache por partilha	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`

Se você quiser…	Em seguida, digite o seguinte…
Ative o BranchCache para todos os compartilhamentos	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Verifique se o modo de operação BranchCache está configurado com a configuração desejada: `vserver cifs branchcache show -vserver vserver_name`

Exemplo

O exemplo a seguir desativa o BranchCache no SVM VS1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Exclua a configuração BranchCache em SVMs

O que acontece quando você exclui a configuração BranchCache

Se você configurou o BranchCache anteriormente, mas não deseja que a máquina virtual de armazenamento (SVM) continue fornecendo conteúdo em cache, você pode excluir a configuração BranchCache no servidor CIFS. Você deve estar ciente do que acontece quando você exclui a configuração.

Quando você exclui a configuração, o ONTAP remove as informações de configuração desse SVM do cluster e interrompe o serviço BranchCache. Você pode escolher se o ONTAP deve excluir o armazenamento de hash no SVM.

A exclusão da configuração BranchCache não interrompe o acesso por clientes habilitados para BranchCache. Depois disso, quando clientes habilitados para BranchCache solicitam informações de metadados sobre conexões SMB existentes para conteúdo que já está em cache, o ONTAP responde com um erro definido pela Microsoft, o que faz com que o cliente envie uma segunda solicitação, solicitando o conteúdo real. Em resposta à solicitação de conteúdo, o servidor CIFS envia o conteúdo real armazenado no SVM

Depois que a configuração do BranchCache é excluída, compartilhamentos SMB não anunciam recursos do BranchCache. Para acessar conteúdo que não foi armazenado em cache anteriormente usando novas conexões SMB, os clientes fazem solicitações de SMB de leitura normais.

Exclua a configuração do BranchCache

O comando que você usa para excluir o serviço BranchCache na máquina virtual de armazenamento (SVM) difere dependendo se você deseja excluir ou manter hashes existentes.

Passo

1. Execute o comando apropriado:

Se você quiser…	Em seguida, digite o seguinte…
Exclua a configuração do BranchCache e exclua hashes existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Exclua a configuração do BranchCache, mas mantenha hashes existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Exemplo

O exemplo a seguir exclui a configuração BranchCache no SVM VS1 e exclui todos os hashes existentes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

O que acontece com BranchCache ao reverter

É importante entender o que acontece quando você reverte o ONTAP para uma versão que não suporte o BranchCache.

- Quando você reverte para uma versão do ONTAP que não suporta BranchCache, os compartilhamentos SMB não anunciam os recursos do BranchCache para clientes habilitados para BranchCache; portanto, os clientes não solicitam informações de hash.

  Em vez disso, eles solicitam o conteúdo real usando solicitações normais de leitura SMB. Em resposta à solicitação de conteúdo, o servidor SMB envia o conteúdo real armazenado na máquina virtual de storage (SVM).

- Quando um nó que hospeda um armazenamento de hash é revertido para uma versão que não suporta BranchCache, o administrador de armazenamento precisa reverter manualmente a configuração do BranchCache usando um comando que é impresso durante a reversão.

  Esse comando exclui a configuração e os hashes do BranchCache.

  Após a conclusão da reversão, o administrador de armazenamento pode excluir manualmente o diretório que continha o armazenamento de hash, se desejado.

Informações relacionadas

Excluindo a configuração BranchCache em SVMs

Melhorar o desempenho de cópia remota da Microsoft

Melhore a visão geral do desempenho de cópia remota da Microsoft

A Microsoft Offloaded Data Transfer (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host.

O ONTAP oferece suporte ao ODX para os protocolos SMB e SAN. A origem pode ser um servidor CIFS ou LUN, e o destino pode ser um servidor CIFS ou LUN.

Em transferências de arquivos não ODX, os dados são lidos da fonte e são transferidos pela rede para o computador cliente. O computador cliente transfere os dados de volta pela rede para o destino. Em resumo, o computador cliente lê os dados da origem e grava-os no destino. Com as transferências de arquivos ODX, os dados são copiados diretamente da origem para o destino.

Como as cópias descarregadas do ODX são realizadas diretamente entre o armazenamento de origem e destino, há benefícios significativos de desempenho. Os benefícios de desempenho obtidos incluem tempo de cópia mais rápido entre a origem e o destino, utilização reduzida de recursos (CPU, memória) no cliente e utilização reduzida da largura de banda de e/S de rede.

Para ambientes SMB, essa funcionalidade só está disponível quando o cliente e o servidor de armazenamento suportam SMB 3,0 e o recurso ODX. Para ambientes SAN, essa funcionalidade só está disponível quando o cliente e o servidor de armazenamento suportam o recurso ODX. Os computadores clientes que suportam ODX e têm o ODX ativado automaticamente e de forma transparente usam transferência de arquivos descarregados ao mover ou copiar arquivos. O ODX é usado independentemente de você arrastar e soltar arquivos através do Windows Explorer ou usar comandos de cópia de arquivo de linha de comando, ou se um aplicativo cliente inicia solicitações de cópia de arquivo.

Informações relacionadas

Melhorar o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática

"Configuração SMB para Microsoft Hyper-V e SQL Server"

Como o ODX funciona

A descarga de cópia ODX usa um mecanismo baseado em token para ler e gravar dados dentro ou entre servidores CIFS habilitados para ODX. Em vez de rotear os dados através do host, o servidor CIFS envia um pequeno token, que representa os dados, para o cliente. O cliente ODX apresenta esse token para o servidor de destino, que então pode transferir os dados representados por esse token da origem para o destino.

Quando um cliente ODX descobre que o servidor CIFS é compatível com ODX, ele abre o arquivo de origem e solicita um token do servidor CIFS. Depois de abrir o arquivo de destino, o cliente usa o token para instruir o servidor a copiar os dados diretamente da origem para o destino.

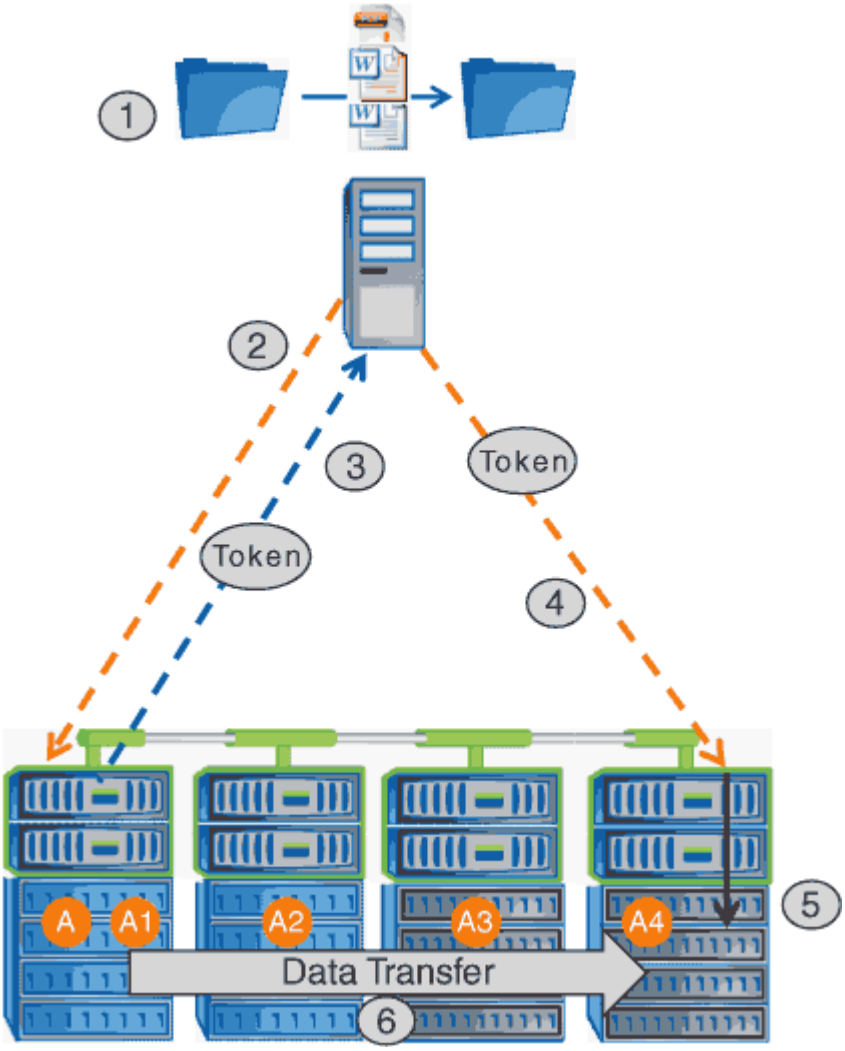
> A origem e o destino podem estar na mesma máquina virtual de storage (SVM) ou em SVMs diferentes, dependendo do escopo da operação de cópia.

O token serve como uma representação pontual dos dados. Como exemplo, quando você copia dados entre locais de armazenamento, um token representando um segmento de dados é retornado ao cliente solicitante, que o cliente copia para o destino, removendo assim a necessidade de copiar os dados subjacentes através

do cliente.

O ONTAP suporta tokens que representam 8 MB de dados. Cópias ODX de mais de 8 MB são executadas usando vários tokens, com cada token representando 8 MB de dados.

A figura a seguir explica as etapas envolvidas com uma operação de cópia ODX:



1. Um usuário copia ou move um arquivo usando o Windows Explorer, uma interface de linha de comando ou como parte de uma migração de máquina virtual, ou um aplicativo inicia cópias ou movimentos de arquivo.
2. O cliente compatível com ODX converte automaticamente essa solicitação de transferência em uma solicitação ODX.

   A solicitação ODX que é enviada para o servidor CIFS contém uma solicitação de um token.

3. Se o ODX estiver habilitado no servidor CIFS e a conexão for sobre SMB 3,0, o servidor CIFS gera um token, que é uma representação lógica dos dados na origem.
4. O cliente recebe um token que representa os dados e os envia com a solicitação de gravação para o servidor CIFS de destino.

   Estes são os únicos dados que são copiados pela rede da origem para o cliente e, em seguida, do cliente para o destino.

5. O token é entregue ao subsistema de armazenamento.
6. O SVM executa a cópia ou a movimentação internamente.

   Se o arquivo copiado ou movido for maior que 8 MB, vários tokens serão necessários para executar a cópia. Passos 2 a 6 conforme executado conforme necessário para concluir a cópia.

> Se houver uma falha com a cópia descarregada do ODX, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação. Da mesma forma, se o servidor CIFS de destino não suportar ODX ou ODX estiver desativado, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Requisitos para usar ODX

Antes de usar o ODX para descarregar cópias com sua máquina virtual de armazenamento (SVM), você precisa estar ciente de certos requisitos.

Requisitos de versão do ONTAP

As versões do ONTAP suportam ODX para descarregamentos de cópias.

Requisitos de versão SMB

- O ONTAP suporta ODX com SMB 3,0 e posterior.
- O SMB 3,0 deve estar habilitado no servidor CIFS antes que o ODX possa ser habilitado:
  - Ativar o ODX também ativa o SMB 3,0, se ele ainda não estiver ativado.
  - Desativar o SMB 3,0 também desativa o ODX.

Requisitos de servidor e cliente do Windows

Antes de poder utilizar o ODX para descarregar cópias, o cliente Windows tem de suportar a funcionalidade.

O "Matriz de interoperabilidade do NetApp"contém as informações mais recentes sobre clientes Windows suportados.

Requisitos de volume

- Os volumes de origem devem ter no mínimo 1,25 GB.
- Se você usar volumes compatados, o tipo de compactação deve ser adaptável e somente o tamanho do grupo de compactação 8K é suportado.

  O tipo de compressão secundária não é suportado.

Diretrizes para o uso do ODX

Antes de poder usar o ODX para descarga de cópia, você precisa estar ciente das diretrizes. Por exemplo, você precisa saber em quais tipos de volumes você pode usar ODX e você precisa entender as considerações do ODX intra-cluster e inter-cluster.

Diretrizes de volume

- Você não pode usar o ODX para descarga de cópia com as seguintes configurações de volume:
  - O tamanho do volume de origem é inferior a 1,25 GB

    O tamanho do volume deve ser de 1,25 GB ou maior para usar o ODX.

  - Volumes só de leitura

    O ODX não é usado para arquivos e pastas residentes em espelhos de compartilhamento de carga ou em volumes de destino SnapMirror ou SnapVault.

  - Se o volume de origem não for desduplicado
- Cópias ODX são suportadas apenas para cópias intra-cluster.

  Não é possível usar o ODX para copiar arquivos ou pastas para um volume em outro cluster.

Outras diretrizes

- Em ambientes SMB, para usar o ODX para descarga de cópia, os arquivos devem ter 256 kb ou mais.

  Arquivos menores são transferidos usando uma operação de cópia tradicional.

- O descarregamento de cópia ODX usa a deduplicação como parte do processo de cópia.

  Se você não quiser que a deduplicação ocorra em volumes SVM ao copiar ou mover dados, desative a descarga de cópia ODX nesse SVM.

- O aplicativo que executa a transferência de dados deve ser escrito para suportar ODX.

  As operações de aplicação que suportam ODX incluem o seguinte:

  - Operações de gerenciamento do Hyper-V, como criar e converter discos rígidos virtuais (VHDs), gerenciar cópias Snapshot e copiar arquivos entre máquinas virtuais
  - Operações do Windows Explorer
  - Comandos de cópia do Windows PowerShell
  - Comandos de cópia do prompt de comando do Windows

    Robocopy no prompt de comando do Windows suporta ODX.

    > Os aplicativos devem estar em execução em servidores Windows ou clientes que suportem ODX.

  +
  Para obter mais informações sobre aplicativos ODX compatíveis em servidores e clientes Windows, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Casos de uso para ODX

Você deve estar ciente dos casos de uso para usar o ODX em SVMs para que você possa determinar em que circunstâncias o ODX fornece benefícios de desempenho.

Os servidores e clientes do Windows que suportam ODX usam a descarga de cópia como a forma padrão de copiar dados em servidores remotos. Se o servidor ou cliente do Windows não suportar ODX ou a descarga de cópia ODX falhar em qualquer ponto, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

- Inter-cluster

  As LUNs de origem e destino estão em volumes diferentes, localizados em nós diferentes, entre clusters. Isso só é suportado para SAN e não funciona para CIFS.

Existem alguns casos de uso especiais adicionais:

- Com a implementação do ONTAP ODX, você pode usar o ODX para copiar arquivos entre compartilhamentos SMB e unidades virtuais conetadas a FC ou iSCSI.

  Você pode usar o Windows Explorer, a CLI do Windows ou PowerShell, Hyper-V ou outras aplicações compatíveis com ODX para copiar ou mover arquivos sem interrupções usando a descarga de cópia ODX entre compartilhamentos SMB e LUNs conetados, desde que os compartilhamentos SMB e LUNs estejam no mesmo cluster.

- O Hyper-V fornece alguns casos de uso adicionais para descarga de cópia ODX:

  - Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB

mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

> Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Ativar ou desativar o ODX

Você pode ativar ou desativar o ODX em máquinas virtuais de armazenamento (SVMs). O padrão é habilitar o suporte para descarga de cópia ODX se o SMB 3,0 também estiver habilitado.

Antes de começar

O SMB 3,0 deve estar ativado.

Sobre esta tarefa

Se você desabilitar o SMB 3,0, o ONTAP também desabilitará o SMB ODX. Se você rehabilitar o SMB 3,0, será necessário reativar manualmente o SMB ODX.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que o descarregamento de cópia ODX seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a descarga de cópia ODX no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Opções de servidor SMB disponíveis

Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática

Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com visão geral de localização automática

A localização automática usa referências de nó automáticas SMB para aumentar a performance do cliente SMB em máquinas virtuais de armazenamento (SVMs). As referências automáticas de nós redirecionam automaticamente o cliente solicitante para um LIF no SVM do nó que hospeda o volume no qual os dados residem, o que pode levar a tempos de resposta aprimorados do cliente.

Quando um cliente SMB se coneta a um compartilhamento SMB hospedado no SVM, ele pode se conetar usando um LIF que está em um nó que não possui os dados solicitados. O nó ao qual o cliente está conetado acessa dados de propriedade de outro nó usando a rede do cluster. O cliente pode ter tempos de resposta mais rápidos se a conexão SMB usar um LIF localizado no nó que contém os dados solicitados:

- O ONTAP fornece essa funcionalidade usando referências do Microsoft DFS para informar clientes SMB que um arquivo ou pasta solicitado no namespace está hospedado em outro lugar.

  Um nó faz uma referência quando determina que há um LIF SVM no nó que contém os dados.

- As referências automáticas de nós são suportadas para endereços IP IPv4 e IPv6 LIF.
- As referências são feitas com base na localização da raiz da partilha através da qual o cliente está ligado.
- A referência ocorre durante a negociação SMB.

  A referência é feita antes da conexão ser estabelecida. Depois que o ONTAP refere o cliente SMB ao nó de destino, a conexão é feita e o cliente acessa os dados através do caminho LIF referido a partir desse ponto. Isso permite que os clientes tenham acesso mais rápido aos dados e evite a comunicação de cluster adicional.

Se um compartilhamento abranger vários pontos de junção e algumas das junções forem para volumes contidos em outros nós, os dados dentro do compartilhamento serão espalhados por vários nós. Como o ONTAP fornece referências locais à raiz do compartilhamento, o ONTAP deve usar a rede de cluster para recuperar os dados contidos nesses volumes não locais. Com esse tipo de arquitetura de namespace, as referências de nó automáticas podem não fornecer benefícios significativos de desempenho.

Se o nó que hospeda os dados não tiver um LIF disponível, o ONTAP estabelece a conexão usando o LIF escolhido pelo cliente. Depois que um arquivo é aberto por um cliente SMB, ele continua a acessar o arquivo através da mesma conexão referida.

Se, por qualquer motivo, o servidor CIFS não puder fazer uma referência, não haverá interrupção no serviço SMB. A conexão SMB é estabelecida como se as referências de nó automáticas não estivessem ativadas.

Informações relacionadas

Melhorando o desempenho de cópia remota da Microsoft

Requisitos e diretrizes para o uso de referências automáticas de nós

Antes de poder usar referências de nó automáticas SMB, também conhecidas como *autolocation*, você precisa estar ciente de certos requisitos, incluindo quais versões do ONTAP suportam o recurso. Você também precisa saber sobre versões de protocolo SMB compatíveis e algumas outras diretrizes especiais.

Requisitos de versão e licença do ONTAP

- Todos os nós no cluster devem estar executando uma versão do ONTAP que suporte referências automáticas de nós.
- Os Widelinks devem estar ativados em um compartilhamento SMB para usar a autenticação automática.
- O CIFS deve ser licenciado e um servidor SMB deve existir nos SVMs. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

Requisitos de versão do protocolo SMB

- Para SVMs, o ONTAP oferece suporte a referências automáticas de nós em todas as versões do SMB.

Requisitos do cliente SMB

Todos os clientes Microsoft suportados pelo ONTAP suportam referências de nó automáticas SMB.

A Matriz de interoperabilidade contém as informações mais recentes sobre quais clientes Windows ONTAP suportam.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos de LIF de dados

Se você quiser usar um data LIF como potencial referência para clientes SMB, crie LIFs de dados com NFS e CIFS habilitados.

As referências automáticas de nós podem falhar ao funcionar se o nó de destino contiver LIFs de dados que

são ativados apenas para o protocolo NFS ou ativados apenas para o protocolo SMB.

Se este requisito não for cumprido, o acesso aos dados não será afetado. O cliente SMB mapeia o compartilhamento usando o LIF original usado pelo cliente para se conetar ao SVM.

Requisitos de autenticação NTLM ao fazer uma conexão SMB referida

A autenticação NTLM deve ser permitida no domínio que contém o servidor CIFS e nos domínios que contêm clientes que desejam usar referências automáticas de nós.

Ao fazer uma referência, o servidor SMB refere um endereço IP ao cliente Windows. Como a autenticação NTLM é usada ao fazer uma conexão usando um endereço IP, a autenticação Kerberos não é executada para conexões referidas.

Isso acontece porque o cliente Windows não pode criar o nome principal do serviço usado pelo Kerberos (que é do formulário `service/NetBIOS name` e `service/FQDN`), o que significa que o cliente não pode solicitar um ticket Kerberos ao serviço.

Diretrizes para o uso de referências automáticas de nós com o recurso de diretório base

Quando os compartilhamentos são configurados com a propriedade de compartilhamento do diretório base ativada, pode haver um ou mais caminhos de pesquisa do diretório base configurados para uma configuração do diretório base. Os caminhos de pesquisa podem apontar para volumes contidos em cada nó que contém volumes SVM. Os clientes recebem uma referência e, se um LIF de dados local ativo estiver disponível, se conetam através de um LIF referido que é local para o diretório home do usuário doméstico.

Há diretrizes quando clientes SMB 1,0 acessam diretórios base dinâmicos com referências automáticas de nós ativadas. Isso ocorre porque os clientes SMB 1,0 exigem a referência automática do nó antes de autenticarem, o que é antes que o servidor SMB tenha o nome do usuário. No entanto, o acesso ao diretório home SMB funciona corretamente para clientes SMB 1,0 se as seguintes instruções forem verdadeiras:

- Os diretórios home SMB são configurados para usar nomes simples, como "%W" (nome de usuário do Windows) ou ""%u" (nome de usuário UNIX mapeado), e não nomes de estilo de nome de domínio, como "%d%W "" (nome de domínio/nome de usuário).
- Ao criar compartilhamentos de diretório base, os nomes de compartilhamentos de diretório base CIFS são configurados com variáveis ("'%W'" ou "'%u'") e não com nomes estáticos, como "'HOME'".

Para clientes SMB 2.x e SMB 3,0, não há diretrizes especiais ao acessar diretórios base usando referências automáticas de nós.

Diretrizes para desabilitar referências automáticas de nós em servidores CIFS com conexões referidas existentes

Se você desativar as referências automáticas de nós depois que a opção tiver sido ativada, os clientes atualmente conetados a um LIF referido mantêm a conexão referida. Como o ONTAP usa referências DFS como o mecanismo para referências de nó automáticas SMB, os clientes podem até se reconetar ao LIF referido depois de desativar a opção até que a referência DFS armazenada em cache do cliente para a conexão referida expire. Isso é verdade mesmo no caso de uma reversão para uma versão do ONTAP que não suporta referências automáticas de nós. Os clientes continuam a usar referências até que o encaminhamento do DFS termine do cache do cliente.

A Autolocation usa referências de nó automáticas SMB para aumentar o desempenho do cliente SMB, referindo os clientes ao LIF no nó que possui o volume de dados de um SVM. Quando um cliente SMB se coneta a um compartilhamento SMB hospedado em um SVM, ele pode se conetar usando um LIF em um nó que não possui os dados solicitados e usa a rede de interconexão de cluster para recuperar dados. O cliente

pode ter tempos de resposta mais rápidos se a conexão SMB usar um LIF localizado no nó que contém os dados solicitados.

O ONTAP fornece essa funcionalidade usando referências do sistema de arquivos distribuídos da Microsoft (DFS) para informar os clientes SMB que um arquivo ou pasta solicitado no namespace está hospedado em outro lugar. Um nó faz uma referência quando determina que há um LIF SVM no nó que contém os dados. As referências são feitas com base na localização da raiz da partilha através da qual o cliente está ligado.

A referência ocorre durante a negociação SMB. A referência é feita antes da conexão ser estabelecida. Depois que o ONTAP refere o cliente SMB ao nó de destino, a conexão é feita e o cliente acessa os dados através do caminho LIF referido a partir desse ponto. Isso permite que os clientes tenham acesso mais rápido aos dados e evite a comunicação de cluster adicional.

Diretrizes para o uso de referências automáticas de nó com clientes Mac os

Os clientes Mac os X não suportam referências de nó automáticas SMB, mesmo que o Mac os suporte o sistema de arquivos distribuídos (DFS) da Microsoft. Os clientes Windows fazem uma solicitação de referência DFS antes de se conetar a um compartilhamento SMB. O ONTAP fornece uma referência a um LIF de dados encontrado no mesmo nó que hospeda os dados solicitados, o que leva a melhores tempos de resposta do cliente. Embora o Mac os suporte DFS, os clientes do Mac os não se comportam exatamente como os clientes do Windows nesta área.

Informações relacionadas

Como o ONTAP ativa diretórios base dinâmicos

"Gerenciamento de rede"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Suporte para referências de nó automáticas SMB

Antes de ativar as referências de nó automático SMB, você deve estar ciente de que certas funcionalidades do ONTAP não suportam referências.

- Os seguintes tipos de volumes não suportam referências de nó automáticas SMB:
  - Membros somente leitura de um espelho de compartilhamento de carga
  - Volume de destino de um espelho de proteção de dados
- As referências de nó não se movem ao lado de uma movimentação de LIF.

  Se um cliente estiver usando uma conexão referida por meio de uma conexão SMB 2.x ou SMB 3,0 e um LIF de dados se mover sem interrupções, o cliente continuará a usar a mesma conexão referida, mesmo que o LIF não seja mais local para os dados.

- As referências de nó não se movem ao lado de uma movimentação de volume.

  Se um cliente estiver usando uma conexão referida em qualquer conexão SMB e ocorrer uma movimentação de volume, o cliente continuará a usar a mesma conexão referida, mesmo que o volume não esteja mais localizado no mesmo nó que o LIF de dados.

Ative ou desative referências de nó automáticas SMB

Você pode habilitar referências de nó automáticas SMB para aumentar o desempenho

de acesso de cliente SMB. Você pode desativar referências automáticas de nós se não quiser que o ONTAP faça referências a clientes SMB.

Antes de começar

Um servidor CIFS deve ser configurado e executado na máquina virtual de storage (SVM).

Sobre esta tarefa

A funcionalidade de referências de nó automático SMB está desativada por predefinição. Você pode ativar ou desativar essa funcionalidade em cada SVM conforme necessário.

Esta opção está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ative ou desative referências de nó automáticas SMB conforme necessário:

Se você quiser que as referências de nó automático SMB sejam…	Digite o seguinte comando…
Ativado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   A configuração de opção entra em vigor para novas sessões SMB. Os clientes com conexão existente podem utilizar referência de nó somente quando o tempo limite de cache existente expirar.

3. Mudar para o nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor SMB disponíveis

Use as estatísticas para monitorar a atividade automática de referência de nós

Para determinar quantas conexões SMB são referidas, você pode monitorar a atividade automática de referência de nó usando o `statistics` comando. Ao monitorar referências, você pode determinar em que medida as referências automáticas estão localizando conexões em nós que hospedam os compartilhamentos e se você deve redistribuir seus LIFs de dados para fornecer melhor acesso local aos compartilhamentos no servidor CIFS.

Sobre esta tarefa

O `cifs` objeto fornece vários contadores no nível de privilégio avançado que são úteis ao monitorar referências automáticas de nó SMB:

- `node_referral_issued`

Número de clientes que receberam uma referência para o nó da raiz de compartilhamento depois que o cliente se conetou usando um LIF hospedado por um nó diferente do nó da raiz de compartilhamento.

- `node_referral_local`

  Número de clientes que se conetaram usando um LIF hospedado pelo mesmo nó que hospeda a raiz de compartilhamento. O acesso local geralmente proporciona um desempenho ideal.

- `node_referral_not_possible`

  Número de clientes que não receberam uma referência para o nó que hospeda a raiz de compartilhamento depois de se conetar usando um LIF hospedado por um nó diferente do nó da raiz de compartilhamento. Isso ocorre porque um LIF de dados ativo para o nó da raiz de compartilhamento não foi encontrado.

- `node_referral_remote`

  Número de clientes que se conetaram usando um LIF hospedado por um nó diferente do nó que hospeda a raiz de compartilhamento. O acesso remoto pode resultar em desempenho degradado.

Você pode monitorar as estatísticas automáticas de referência de nós na sua máquina virtual de storage (SVM) coletando e visualizando dados para um período de tempo específico (uma amostra). Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências de desempenho.

Para avaliar e usar as informações que você coleta a partir do `statistics` comando, você deve entender a distribuição de clientes em seus ambientes.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Visualize estatísticas automáticas de referência de nó usando o `statistics` comando.

   Este exemplo exibe estatísticas automáticas de referência de nó coletando e visualizando dados para um período de tempo de amostragem:

   a. Inicie a coleção: `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. Aguarde até que o tempo de recolha pretendido decorra.

   c. Parar a coleção: `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   d. Veja as estatísticas automáticas de referência de nó: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

A saída exibe contadores para todos os nós participantes do SVM VS1. Para maior clareza, apenas os campos de saída relacionados às estatísticas automáticas de referência de nó são fornecidos no exemplo.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Exibindo estatísticas

"Configuração do monitoramento de desempenho"

Monitore informações de referência automática de nós SMB no lado do cliente usando um cliente Windows

Para determinar quais referências são feitas da perspetiva do cliente, você pode usar o utilitário Windows `dfsutil.exe`.

O kit RSAT (Remote Server Administration Tools) disponível com o Windows 7 e clientes posteriores contém o `dfsutil.exe` utilitário. Usando este utilitário, você pode exibir informações sobre o conteúdo do cache de referência, bem como visualizar informações sobre cada referência que o cliente está usando atualmente. Você também pode usar o utilitário para limpar o cache de referência do cliente. Para obter mais informações, consulte a Microsoft TechNet Library.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Forneça segurança de pastas em compartilhamentos com enumeração baseada em acesso

Forneça segurança de pastas em compartilhamentos com visão geral de enumeração baseada em acesso

Quando a enumeração baseada em acesso (ABE) está ativada em um compartilhamento SMB, os usuários que não têm permissão para acessar uma pasta ou arquivo contido no compartilhamento (seja por restrições de permissão individuais ou de grupo) não veem esse recurso compartilhado exibido em seu ambiente, embora o próprio compartilhamento permaneça visível.

As propriedades de compartilhamento convencionais permitem especificar quais usuários (individualmente ou em grupos) têm permissão para exibir ou modificar arquivos ou pastas contidos no compartilhamento. No entanto, eles não permitem que você controle se pastas ou arquivos dentro do compartilhamento são visíveis para usuários que não têm permissão para acessá-los. Isso pode causar problemas se os nomes dessas pastas ou arquivos dentro do compartilhamento descreverem informações confidenciais, como os nomes de clientes ou produtos em desenvolvimento.

A enumeração baseada em acesso (ABE) estende as propriedades de compartilhamento para incluir a enumeração de arquivos e pastas dentro do compartilhamento. Portanto, O ABE permite filtrar a exibição de arquivos e pastas dentro do compartilhamento com base nos direitos de acesso do usuário. Ou seja, o compartilhamento em si seria visível para todos os usuários, mas os arquivos e pastas dentro do compartilhamento poderiam ser exibidos ou ocultados de usuários designados. Além de proteger informações confidenciais em seu local de trabalho, o ABE permite simplificar a exibição de grandes estruturas de diretórios para benefício dos usuários que não precisam acessar toda a sua gama de conteúdo. Por exemplo, o compartilhamento em si seria visível para todos os usuários, mas arquivos e pastas dentro do compartilhamento poderiam ser exibidos ou ocultos.

Saiba mais "Impacto no desempenho ao usar enumeração baseada em acesso SMB/CIFS"sobre .

Ative ou desative a enumeração baseada em acesso em compartilhamentos SMB

Você pode ativar ou desativar a enumeração baseada em acesso (ABE) em compartilhamentos SMB para permitir ou impedir que os usuários vejam recursos compartilhados que eles não têm permissão para acessar.

Sobre esta tarefa

Por padrão, o ABE está desativado.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ative o ABE em um novo compartilhamento	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Você pode especificar configurações de compartilhamento opcionais adicionais e propriedades de compartilhamento adicionais ao criar um compartilhamento SMB. Para obter mais informações, consulte a página man para o `vserver cifs share create` comando.
Ative o ABE em um compartilhamento existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` As propriedades de compartilhamento existentes são preservadas. A propriedade ABE Share é adicionada à lista existente de propriedades de ações.
Desative o ABE em um compartilhamento existente	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Outras propriedades de compartilhamento são preservadas. Somente a propriedade ABE Share é removida da lista de propriedades de compartilhamento.

2. Verifique se a configuração de compartilhamento está correta usando o `vserver cifs share show` comando.

Exemplos

O exemplo a seguir cria um compartilhamento ABE SMB chamado "vendas" com um caminho de `/sales` no SVM VS1. A ação é criada com `access-based-enumeration` como uma propriedade de ação:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
            Share Properties: access-based-enumeration
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

O exemplo a seguir adiciona a `access-based-enumeration` propriedade share a um compartilhamento SMB chamado "ata2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Informações relacionadas

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Ativar ou desativar a enumeração baseada em acesso a partir de um cliente Windows

Você pode ativar ou desativar a enumeração baseada em acesso (ABE) em compartilhamentos SMB de um cliente Windows, o que permite configurar essa configuração de compartilhamento sem precisar se conetar ao servidor CIFS.

O `abecmd` utilitário não está disponível em novas versões dos clientes Windows Server e Windows. Foi lançado como parte do Windows Server 2008. O suporte terminou para o Windows Server 2008 em 14 de janeiro de 2020.

Passos

1. Em um cliente Windows que suporte ABE, digite o seguinte comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Para obter mais informações sobre o `abecmd` comando, consulte a documentação do cliente Windows.

Dependências de nomes de arquivos e diretórios NFS e SMB

Visão geral das dependências de nomes de arquivos e diretórios NFS e SMB

As convenções de nomenclatura de arquivos e diretórios dependem tanto dos sistemas operacionais dos clientes de rede quanto dos protocolos de compartilhamento de arquivos, além das configurações de idioma do cluster e dos clientes do ONTAP.

O sistema operacional e os protocolos de compartilhamento de arquivos determinam o seguinte:

- Carateres que um nome de arquivo pode usar
- Sensibilidade em caso de um nome de ficheiro

O ONTAP suporta carateres multibyte em nomes de arquivo, diretório e qtree, dependendo da versão do ONTAP.

Carateres que um nome de arquivo ou diretório pode usar

Se você estiver acessando um arquivo ou diretório de clientes com sistemas operacionais diferentes, use carateres válidos em ambos os sistemas operacionais.

Por exemplo, se você usar UNIX para criar um arquivo ou diretório, não use dois pontos (:) no nome porque os dois pontos não são permitidos em nomes de arquivo ou diretório MS-dos. Como as restrições em carateres válidos variam de um sistema operacional para outro, consulte a documentação do sistema operacional cliente para obter mais informações sobre carateres proibidos.

Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo

Os nomes de arquivos e diretórios são sensíveis a maiúsculas e minúsculas para clientes NFS, mas que preservam casos para clientes SMB. Você deve entender quais são as implicações em um ambiente multiprotocolo e as ações que pode precisar tomar ao especificar o caminho ao criar compartilhamentos SMB e ao acessar dados nos compartilhamentos.

Se um cliente SMB criar um diretório `testdir` chamado , os clientes SMB e NFS exibirão o nome do arquivo como `testdir`. No entanto, se um usuário SMB tentar criar um nome de diretório mais tarde `TESTDIR` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar posteriormente um diretório `TESTDIR` chamado , clientes NFS e SMB exibirão o nome do diretório de maneira diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de diretório à medida que foram criados, por `testdir` exemplo e `TESTDIR`, porque os nomes de diretório são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois diretórios. Um diretório tem o nome do arquivo base. Os diretórios adicionais recebem um nome de arquivo 8,3.
  - Em clientes SMB, você verá `testdir` e `TESTDI~1`.
  - O ONTAP cria o `TESTDI~1` nome do diretório para diferenciar os dois diretórios.

    Nesse caso, você deve usar o nome 8,3 ao especificar um caminho de compartilhamento ao criar ou modificar um compartilhamento em uma máquina virtual de storage (SVM).

Da mesma forma para arquivos, se um cliente SMB criar `test.txt`, os clientes SMB e NFS exibirão o nome do arquivo como `text.txt`. No entanto, se um usuário SMB tentar criar mais tarde `Test.txt` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar mais tarde um arquivo `Test.txt` chamado , clientes NFS e SMB exibirão o nome do arquivo de forma diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de arquivos à medida que foram criados e `test.txt` `Test.txt` , porque os nomes de arquivos são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois arquivos. Um arquivo tem o nome do arquivo base. Os ficheiros adicionais recebem um nome de ficheiro 8,3.
  - Em clientes SMB, você verá `test.txt` e `TEST~1.TXT`.
  - O ONTAP cria o `TEST~1.TXT` nome do arquivo para diferenciar os dois arquivos.

> Se você tiver ativado ou modificado o mapeamento de carateres usando os comandos SVM CIFS de mapeamento de carateres, uma pesquisa Windows normalmente insensível a maiúsculas e minúsculas torna-se sensível a maiúsculas e minúsculas.

Como o ONTAP cria nomes de arquivo e diretório

O ONTAP cria e mantém dois nomes para arquivos ou diretórios em qualquer diretório que tenha acesso de um cliente SMB: O nome longo original e um nome no formato 8,3.

Para nomes de arquivo ou diretório que excedam o nome de oito carateres ou o limite de extensão de três carateres (para arquivos), o ONTAP gera um nome de formato 8,3 da seguinte forma:

- Ele trunca o nome do arquivo ou diretório original para seis carateres, se o nome exceder seis carateres.
- Ele adiciona um til (…) e um número, um a cinco, aos nomes de arquivo ou diretório que não são mais exclusivos depois de serem truncados.

  Se ele ficar sem números porque há mais de cinco nomes semelhantes, ele cria um nome exclusivo que não tem relação com o nome original.

- No caso dos arquivos, ele trunca a extensão do nome do arquivo para três carateres.

Por exemplo, se um cliente NFS criar um arquivo chamado `specifications.html`, o nome do arquivo de formato 8,3 criado pelo ONTAP será `specif~1.htm`. Se esse nome já existir, o ONTAP usará um número diferente no final do nome do arquivo. Por exemplo, se um cliente NFS criar outro arquivo chamado `specifications_new.html`, o formato 8,3 do `specifications_new.html` é `specif~2.htm`.

Como o ONTAP lida com nomes de arquivos, diretórios e qtree de vários bytes

Começando com ONTAP 9.5, o suporte para nomes codificados UTF-8 de 4 bytes permite a criação e exibição de nomes de arquivos, diretórios e árvores que incluem carateres suplementares Unicode fora do plano multilíngue básico (BMP). Em versões anteriores, esses carateres suplementares não foram exibidos corretamente em ambientes multiprotocolo.

Para ativar o suporte para nomes codificados UTF-8 de 4 bytes, um novo código de linguagem *utf8mb4* está disponível para as `vserver` famílias de comandos e `volume` .

Você deve criar um novo volume de uma das seguintes maneiras:

- Definir a opção de volume `-language` explicitamente: `volume create -language utf8mb4 {…}`
- Herdando a opção de volume `-language` de uma SVM que foi criada ou modificada para a opção: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- No ONTAP 9.6 e anteriores, não é possível modificar volumes existentes para suporte a utf8mb4; é necessário criar um novo volume pronto para utf8mb4 e migrar os dados usando ferramentas de cópia baseadas em cliente.

  Você pode atualizar SVMs para suporte a utf8mb4, mas os volumes existentes mantêm seus códigos de idioma originais.

  Se você estiver usando o ONTAP 9.7P1 ou posterior, poderá modificar volumes existentes para o utf8mb4 com uma solicitação de suporte. Para obter mais informações, "O idioma do volume pode ser alterado após a criação no ONTAP?"consulte .

- Começando com ONTAP 9.8, você pode usar o `[-language <Language code>]` parâmetro para alterar o idioma do volume de *.UTF-8 para utf8mb4. Para alterar o idioma de um volume, "Suporte à NetApp"contacte .

  Nomes LUN com carateres UTF-8 de 4 bytes não são suportados atualmente.

- Os dados de carateres Unicode são normalmente representados em aplicações de sistemas de ficheiros Windows utilizando o formato de transformação Unicode de 16 bits (UTF-16) e em sistemas de ficheiros NFS utilizando o formato de transformação Unicode de 8 bits (UTF-8).

  Em versões anteriores ao ONTAP 9.5, nomes incluindo carateres suplementares UTF-16 que foram criados por clientes Windows foram exibidos corretamente para outros clientes Windows, mas não foram traduzidos corretamente para UTF-8 para clientes NFS. Da mesma forma, nomes com carateres suplementares UTF-8 por clientes NFS criados não foram traduzidos corretamente para UTF-16 para clientes Windows.

- Quando você cria nomes de arquivo em sistemas que executam o ONTAP 9.4 ou anteriores que contêm carateres suplementares válidos ou inválidos, o ONTAP rejeita o nome do arquivo e retorna um erro de nome de arquivo inválido.

  Para evitar esse problema, use apenas carateres BMP em nomes de arquivo e evite usar carateres suplementares ou atualize para o ONTAP 9.5 ou posterior.

Começando com ONTAP 9, carateres Unicode são permitidos em nomes de qtree.

- Você pode usar a `volume qtree` família de comandos ou o System Manager para definir ou modificar nomes de qtree.
- Os nomes de qtree podem incluir carateres de vários bytes no formato Unicode, como carateres japoneses e chineses.
- Em versões anteriores ao ONTAP 9.5, apenas os carateres BMP (ou seja, aqueles que poderiam ser representados em 3 bytes) foram suportados.

> Em versões anteriores ao ONTAP 9.5, o caminho de junção do volume pai da qtree pode conter nomes de qtree e diretório com carateres Unicode. O `volume show` comando exibe esses nomes corretamente quando o volume pai tem uma configuração de idioma UTF-8. No entanto, se o idioma do volume pai não for uma das configurações de idioma UTF-8, algumas partes do caminho de junção serão exibidas usando um nome alternativo NFS numérico.

- Em versões 9,5 e posteriores, os carateres de 4 bytes são suportados em nomes de qtree, desde que a qtree esteja em um volume habilitado para utf8mb4.

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Os clientes NFS podem criar nomes de arquivos que contêm carateres que não são válidos para clientes SMB e determinados aplicativos do Windows. Você pode configurar o mapeamento de carateres para a tradução de nome de arquivo em volumes para permitir que clientes SMB acessem arquivos com nomes NFS que, de outra forma, não seriam válidos.

Sobre esta tarefa

Quando os arquivos criados por clientes NFS são acessados por clientes SMB, o ONTAP examina o nome do arquivo. Se o nome não for um nome de arquivo SMB válido (por exemplo, se ele tiver um caractere de dois pontos "':'" incorporado), o ONTAP retornará o nome de arquivo 8,3 que é mantido para cada arquivo. No entanto, isso causa problemas para aplicativos que codificam informações importantes em nomes de arquivos longos.

Portanto, se você estiver compartilhando um arquivo entre clientes em sistemas operacionais diferentes, você deve usar carateres nos nomes de arquivo que são válidos em ambos os sistemas operacionais.

No entanto, se você tiver clientes NFS que criam nomes de arquivo contendo carateres que não são nomes de arquivo válidos para clientes SMB, você poderá definir um mapa que converte os carateres NFS inválidos em carateres Unicode que tanto SMB quanto determinados aplicativos do Windows aceitam. Por exemplo, essa funcionalidade suporta os aplicativos CATIA MCAD e Mathematica, bem como outros aplicativos que têm esse requisito.

Você pode configurar o mapeamento de carateres em uma base volume por volume.

Você deve ter em mente o seguinte ao configurar o mapeamento de carateres em um volume:

- O mapeamento de carateres não é aplicado em pontos de junção.

  Você deve configurar explicitamente o mapeamento de carateres para cada volume de junção.

- Você deve certificar-se de que os carateres Unicode que são usados para representar carateres inválidos ou ilegais são carateres que normalmente não aparecem em nomes de arquivos; caso contrário, mapeamentos indesejados ocorrem.

Por exemplo, se você tentar mapear dois pontos (:) para um hífen (-), mas o hífen (-) foi usado no nome do arquivo corretamente, um cliente Windows tentando acessar um arquivo chamado "'a-b'" teria sua solicitação mapeada para o nome NFS de "'a:b'" (não o resultado desejado).

- Depois de aplicar o mapeamento de carateres, se o mapeamento ainda contiver um caractere Windows inválido, o ONTAP volta para os nomes de arquivos do Windows 8,3.
- Em notificações FPolicy, logs de auditoria nas e mensagens de rastreamento de segurança, os nomes de arquivo mapeados são exibidos.
- Quando uma relação SnapMirror do tipo DP é criada, o mapeamento de carateres do volume de origem não é replicado no volume DP de destino.
- Sensibilidade do caso: Como os nomes mapeados do Windows se transformam em nomes NFS, a pesquisa dos nomes segue semântica de NFS. Isso inclui o fato de que pesquisas NFS são sensíveis a maiúsculas e minúsculas. Isso significa que os aplicativos que acessam compartilhamentos mapeados não devem depender de comportamento insensível a maiúsculas e minúsculas do Windows. No entanto, o nome 8,3 está disponível, e isso é insensível a maiúsculas e minúsculas.
- Mapeamentos parciais ou inválidos: Depois de mapear um nome para retornar aos clientes fazendo enumeração de diretórios ("dir"), o nome Unicode resultante é verificado para a validade do Windows. Se esse nome ainda tiver carateres inválidos nele, ou se for inválido para o Windows (por exemplo, termina em "." ou em branco), o nome 8,3 será retornado em vez do nome inválido.

Passo

1. Configurar mapeamento de carateres

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` E

O mapeamento consiste em uma lista de pares de carateres fonte-alvo separados por "':'". Os carateres são carateres Unicode inseridos usando dígitos hexadecimais. Por exemplo: 3c:E03C. E

O primeiro valor de cada `mapping_text` par que é separado por dois pontos é o valor hexadecimal do caractere NFS que você deseja traduzir, e o segundo valor é o valor Unicode que SMB usa. Os pares de mapeamento devem ser únicos (deve existir um mapeamento um-para-um).

- Mapeamento de origem

A tabela a seguir mostra o conjunto de carateres Unicode permissível para mapeamento de fontes:

E

Caractere Unicode	Caráter impresso	Descrição
0x01-0x19	Não aplicável	Caracteres de controle não-impressão
0x5C		Barra invertida
0x3A	:	Cólon
0x2A	*	Asterisco

Caractere Unicode	Caráter impresso	Descrição
0x3F	?	Ponto de interrogação
0x22	"	Marca de cotação
0x3C	*	Menos de
0x3E	>	Superior a.
0x7C		
Linha vertical	0xB1	±

- Mapeamento de alvos

  Você pode especificar carateres de destino na ""Área de uso privado"" do Unicode no seguinte intervalo: U-E0000…U-F8FF.

Exemplo

O comando a seguir cria um mapeamento de carateres para um volume chamado "data" na máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Informações relacionadas

Criação e gerenciamento de volumes de dados em namespaces nas

Comandos para gerenciar mapeamentos de carateres para a tradução de nome de arquivo SMB

É possível gerenciar o mapeamento de carateres criando, modificando, exibindo informações ou excluindo mapeamentos de carateres de arquivo usados para a tradução de nomes de arquivo SMB em volumes FlexVol.

Se você quiser…	Use este comando…
Criar novos mapeamentos de carateres de arquivo	`vserver cifs character-mapping create`
Exibir informações sobre mapeamentos de carateres de arquivo	`vserver cifs character-mapping show`

Se você quiser…	Use este comando…
Modificar mapeamentos de carateres de arquivo existentes	`vserver cifs character-mapping modify`
Excluir mapeamentos de carateres de arquivo	`vserver cifs character-mapping delete`

Para obter mais informações, consulte a página man para cada comando.

Informações relacionadas

Configurando o mapeamento de carateres para a tradução de nome de arquivo SMB em volumes

Fornecer acesso de cliente S3 aos dados nas

Suporte multiprotocolo S3 no ONTAP

A partir do ONTAP 9.12,1, é possível permitir que os clientes que executam o protocolo S3 acessem os mesmos dados que estão sendo atendidos aos clientes que usam os protocolos NFS e SMB sem reformatação. Esse recurso permite que os dados nas continuem sendo servidos a clientes nas, enquanto apresentam dados de objetos a clientes S3 que executam aplicações S3 (como data mining e inteligência artificial).

A funcionalidade multiprotocolo S3 aborda dois casos de uso:

1. Acesso a dados nas existentes usando clientes S3

   Se os dados existentes tiverem sido criados usando clientes nas tradicionais (NFS ou SMB) e estiverem localizados em volumes nas (volumes FlexVol ou FlexGroup), agora você poderá usar ferramentas de análise em clientes do S3 para acessar esses dados.

2. Storage de back-end para clientes modernos com capacidade para executar e/S usando protocolos nas e S3

   Agora você pode fornecer acesso integrado para aplicativos como Spark e Kafka que podem ler e gravar os mesmos dados usando protocolos nas e S3.

Como funciona o suporte multiprotocolo S3

O suporte multiprotocolo ONTAP permite que você apresente o mesmo conjunto de dados que uma hierarquia de arquivos ou objetos em um bucket. Para fazer isso, o ONTAP cria "S3 buckets nas" que permitem que os clientes do S3 criem, leiam, excluam e enumerem arquivos no storage nas usando solicitações de objetos do S3. Este mapeamento está em conformidade com a configuração de segurança nas, observando permissões de acesso a arquivos e diretórios, bem como gravar na trilha de auditoria de segurança, conforme necessário.

Esse mapeamento é realizado apresentando uma hierarquia de diretórios nas especificada como um bucket S3. Cada arquivo na hierarquia de diretórios é representado como um objeto S3 cujo nome é relativo do diretório mapeado para baixo, com limites de diretório representados pelo caractere de barra ('/').

Os usuários do S3 definidos pela ONTAP podem acessar esse storage, conforme governado pelas políticas de bucket definidas para o bucket que é mapeado para o diretório nas. Para que isso seja possível, mapeamentos devem ser definidos entre os usuários S3 e os usuários SMB/NFS. As credenciais do usuário

SMB/NFS serão usadas para a verificação de permissões nas e incluídas em todos os Registros de auditoria resultantes desses acessos.

Quando criado por clientes SMB ou NFS, um arquivo é colocado imediatamente em um diretório e, portanto, visível para clientes, antes que qualquer dado seja gravado nele. Os clientes S3 esperam semântica diferente, na qual o novo objeto não é visível no namespace até que todos os seus dados tenham sido escritos. Esse mapeamento do S3 para o armazenamento nas cria arquivos usando semântica S3, mantendo os arquivos invisíveis externamente até que o comando de criação S3 seja concluído.

Proteção de dados para buckets do nas S3

S3 "buckets" nas são simplesmente mapeamentos de dados nas para clientes S3, e não são buckets do S3 padrão. Portanto, não há necessidade de proteger buckets do nas S3 usando a funcionalidade do NetApp SnapMirror S3. Em vez disso, você pode proteger volumes que contêm S3 buckets do nas usando a replicação de volume assíncrona do SnapMirror. A recuperação de desastres síncrona SnapMirror e SVM não é compatível.

A partir do ONTAP 9.14,1, os buckets nas de S3 GB são compatíveis com agregados espelhados e sem espelhamento para configurações MetroCluster IP e FC.

Saiba mais "Assíncrono com SnapMirror"sobre .

Auditoria para buckets do nas S3

Como os buckets do nas S3 não são buckets do S3 convencionais, a auditoria do S3 não pode ser configurada para auditar o acesso neles. Saiba mais "Auditoria S3"sobre o .

No entanto, os arquivos e diretórios nas mapeados em buckets do nas S3 podem ser auditados para eventos de acesso usando procedimentos de auditoria convencionais do ONTAP. As operações S3 podem, portanto, acionar eventos de auditoria nas, com as seguintes exceções:

- Se o acesso de cliente S3 for negado pela configuração de diretiva S3 (política de grupo ou bucket), a auditoria nas para o evento não será iniciada. Isso ocorre porque as permissões do S3 são verificadas antes que as verificações de auditoria SVM possam ser feitas.
- Se o arquivo de destino de uma solicitação de S3 GET for de tamanho 0, o conteúdo 0 será retornado à solicitação de GET e o acesso de leitura não será registrado.
- Se o arquivo de destino de uma solicitação de S3 GET estiver em uma pasta para a qual o usuário não tenha permissão de avanço, a tentativa de acesso falhará e o evento não será registrado.

Saiba mais "Auditoria de eventos nas em SVMs"sobre .

Upload multipart de objeto

A partir do ONTAP 9.16,1, o upload de várias partes de objetos é suportado quando "balanceamento de capacidade avançado" o FlexGroup volumes está ativado.

O upload multipart de objeto no armazenamento de arquivos nas permite que um cliente de protocolo S3 carregue um objeto grande como partes menores. O upload de várias partes do objeto tem os seguintes benefícios:

- Ele permite que objetos sejam carregados em paralelo.
- Em caso de falha ou pausa no upload, apenas as partes que ainda não foram carregadas precisarão ser carregadas. O upload de todo o objeto não precisa ser reiniciado.

- Se o tamanho do objeto não for conhecido antecipadamente (por exemplo, quando um objeto grande ainda está sendo escrito), os clientes podem começar a carregar partes do objeto imediatamente e concluir o upload após o objeto inteiro ter sido criado.

O upload multipart suporta as seguintes ações S3:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Interoperabilidade do S3 e nas

Os buckets do ONTAP S3 nas suportam a funcionalidade nas e S3 padrão, exceto conforme listado aqui.

Funcionalidade nas atualmente não suportada por buckets do nas S3

Camada de capacidade do FabricPool

Os buckets do nas S3 não podem ser configurados como uma camada de capacidade para o FabricPool.

Funcionalidade S3 não suportada atualmente por buckets do nas S3

Metadados de usuários da AWS

- Os pares de valores-chave recebidos como parte dos metadados de usuário do S3 não são armazenados no disco juntamente com os dados de objeto na versão atual.
- Cabeçalhos de solicitação com o prefixo "x-amz-meta" são ignorados.

Tags da AWS

- Em pedidos PUT object e Multipart Initiate, cabeçalhos com o prefixo "x-amz-tagging" são ignorados.
- As solicitações para atualizar tags em um arquivo existente (ou seja, um put, get e Delete Requests com a string de consulta ?tagging) são rejeitadas com um erro.

Controle de versão

Não é possível especificar o controle de versão na configuração de mapeamento de bucket.

- Solicitações que incluem especificações de versão não null (a query-string) recebem respostas de erro.
- As solicitações para afetar o estado de controle de versão de um bucket são rejeitadas com erros.

Requisitos de dados nas para acesso ao cliente S3

É importante entender que existem algumas incompatibilidades inerentes ao mapeamento de arquivos e diretórios nas para acesso S3. Pode ser necessário ajustar hierarquias de arquivos nas antes de servi-los usando buckets do nas S3.

Um bucket do S3 nas fornece acesso S3 a um diretório nas mapeando esse diretório usando a sintaxe do bucket do S3, e os arquivos na árvore de diretórios são vistos como objetos. Os nomes de objeto são os nomes de caminho delimitados por barra dos arquivos em relação ao diretório especificado na configuração de bucket S3.

Esse mapeamento impõe alguns requisitos quando arquivos e diretórios são servidos usando buckets do nas

S3:

- Os nomes S3 são limitados a 1024 bytes, portanto os arquivos com pathnames mais longos não são acessíveis usando S3.
- Os nomes de arquivo e diretório estão limitados a 255 carateres, portanto, um nome de objeto não pode ter mais de 255 carateres consecutivos sem barra ('/')
- Um nome de caminho SMB delimitado por carateres de barra invertida ('") aparecerá em S3 como um nome de objeto contendo carateres de barra direta ('/') em vez disso.
- Alguns pares de nomes de objetos S3 legais não podem coexistir na árvore de diretórios nas mapeada. Por exemplo, os nomes de objetos S3 legais "part1/part2" e "part1/part2/part3" mapeiam para arquivos que não podem existir simultaneamente na árvore de diretórios nas, pois "part1/part2" é um arquivo no primeiro nome e um diretório no outro.
  - Se "part1/part2" for um arquivo existente, uma criação S3 de "part1/part2/part3" falhará.
  - Se "part1/part2/part3" for um arquivo existente, uma criação ou exclusão S3 de "part1/part2" falhará.
  - Uma criação de objeto S3 que corresponde ao nome de um objeto existente substitui o objeto pré-existente (em buckets não versionados); que se mantém no nas, mas requer uma correspondência exata. Os exemplos acima não causarão a remoção do objeto existente porque enquanto os nomes colidem, eles não coincidem.

Embora um armazenamento de objetos seja projetado para suportar um número muito grande de nomes arbitrários, uma estrutura de diretório nas pode experimentar problemas de desempenho se um número muito grande de nomes for colocado em um diretório. Em particular, nomes sem carateres de barra ('/') serão todos colocados no diretório raiz do mapeamento nas. As aplicações que fazem uso extensivo de nomes que não são "amigáveis ao nas" seriam mais bem hospedadas em um bucket de armazenamento de objetos real em vez de um mapeamento nas.

Habilite o acesso de protocolo S3 a dados nas

A habilitação do acesso ao protocolo S3 consiste em garantir que um SVM habilitado para nas atenda aos mesmos requisitos que um servidor habilitado para S3, incluindo a adição de um servidor de armazenamento de objetos e a verificação dos requisitos de rede e autenticação.

Para novas instalações do ONTAP, é recomendável habilitar o acesso de protocolo S3 a um SVM depois de configurá-lo para fornecer dados nas aos clientes. Para saber mais sobre a configuração do protocolo nas, consulte:

- "Configuração NFS"
- "Configuração SMB"

Antes de começar

É necessário configurar o seguinte antes de ativar o protocolo S3:

- O protocolo S3 e os protocolos nas desejados - NFS, SMB ou ambos - são licenciados.
- Um SVM é configurado para os protocolos nas desejados.
- Existem servidores NFS e/ou SMB.
- DNS e quaisquer outros serviços necessários estão configurados.
- Os dados nas estão sendo exportados ou compartilhados para sistemas cliente.

Sobre esta tarefa

Um certificado de autoridade de certificação (CA) é necessário para habilitar o tráfego HTTPS de clientes S3 para o SVM habilitado para S3. Os certificados CA de três fontes podem ser usados:

- Um novo certificado auto-assinado da ONTAP no SVM.
- Certificado auto-assinado existente do ONTAP no SVM.
- Um certificado de terceiros.

Você pode usar os mesmos LIFs de dados para o bucket do S3/nas que você usa para fornecer dados nas. Se forem necessários endereços IP específicos, "Crie LIFs de dados"consulte . Uma política de dados de serviço do S3 é necessária para habilitar o tráfego de dados do S3 nos LIFs. Você pode modificar a política de serviços existente da SVM para incluir o S3.

Quando você cria o servidor de objetos S3, você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN do servidor S3 não deve começar com um nome de bucket.

System Manager

1. Habilite o S3 em uma VM de storage com protocolos nas configurados.
   a. Clique em **armazenamento > armazenamento VMs**, selecione uma VM de armazenamento pronta para nas, clique em Configurações e, em seguida, clique em S3.
   b. Selecione o tipo de certificado. Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.
   c. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Verifique se o protocolo S3 é permitido no SVM
   `vserver show -fields allowed-protocols`
2. Registre o certificado de chave pública deste SVM. Se for necessário um novo certificado auto-assinado do ONTAP, "Crie e instale um certificado de CA no SVM"consulte .
3. Atualize a política de dados de serviço
   a. Exibir a política de dados de serviço do SVM
      `network interface service-policy show -vserver svm_name`
   b. Adicione o `data-core` e `data-s3-server services` se não estiverem presentes. E
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Verifique se as LIFs de dados no SVM atendem aos seus requisitos
   `network interface show -vserver svm_name`
5. Crie o servidor S3
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Você pode especificar opções adicionais ao criar o servidor S3 ou a qualquer momento mais tarde.

- O HTTPS é ativado por padrão na porta 443. Você pode alterar o número da porta com a opção -secure-listener-port. Quando o HTTPS está ativado, os certificados de CA são necessários para uma integração adequada com SSL/TLS. A partir do ONTAP 9.15,1, o TLS 1,3 é compatível com armazenamento de objetos S3.
- O HTTP está desativado por padrão; quando ativado, o servidor escuta na porta 80. Você pode ativá-lo com a opção -is-http-enabled ou alterar o número da porta com a opção -listener-port. Quando o HTTP está ativado, todas as solicitações e respostas são enviadas pela rede em texto não criptografado.

1. Verifique se S3 está configurado como desejado
   `vserver object-store-server show`

O seguinte comando verifica os valores de configuração de todos os servidores de armazenamento de objetos

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Crie um bucket do nas S3

Um buckets do nas S3 é um mapeamento entre um nome de bucket do S3 e um caminho nas. Os buckets nas do S3 permitem que você forneça acesso S3 a qualquer parte do namespace SVM com volumes e estrutura de diretórios existentes.

Antes de começar

- Um servidor de objetos S3 é configurado em uma SVM que contém dados nas.
- Os dados nas estão em conformidade com a "Requisitos para acesso ao cliente S3".

Sobre esta tarefa

Você pode configurar buckets do S3 nas para especificar qualquer conjunto de arquivos e diretórios no diretório raiz do SVM.

Você também pode definir políticas de bucket que permitem ou não permitem o acesso aos dados do nas com base em qualquer combinação desses parâmetros:

- Arquivos e diretórios
- Permissões de usuário e grupo
- S3 operações

Por exemplo, você pode querer políticas de bucket separadas que concedem acesso somente leitura a um grande grupo de usuários e outra que permita que um grupo limitado execute operações em um subconjunto desses dados.

Como os "buckets" do nas S3 são mapeamentos e não buckets do S3, as seguintes propriedades dos buckets do S3 padrão não se aplicam aos buckets do nas S3.

- * aggr-list-multiplicador / storage-Service-level / volume / exclude-aggr-list / qos-policy-group * não são criados volumes ou qtree ao configurar buckets do S3 nas.
- **A função é -protegida/está -protegida/está -protegida-na-ONTAP** mais de S3 buckets nas não são protegidos ou espelhados usando o SnapMirror S3, mas em vez disso estarão usando a proteção

SnapMirror regular disponível na granularidade do volume.

- **Os volumes nas de estado de versionamento** geralmente têm a tecnologia Snapshot disponível para salvar versões diferentes. No entanto, o controle de versão não está disponível atualmente em buckets do nas S3.
- *As estatísticas equivalentes usadas em lógica estão disponíveis para volumes nas através dos comandos de volume.

System Manager

Adicione um novo bucket do S3 nas em uma VM de storage habilitada para nas.

1. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
2. Insira um nome para o bucket do nas S3 e selecione a VM de armazenamento, não insira um tamanho e clique em **mais Opções**.
3. Introduza um nome de caminho válido ou clique em Procurar para selecionar a partir de uma lista de nomes de caminho válidos. Quando você insere um pathname válido, as opções que não são relevantes para a configuração do nas S3 são ocultadas.
4. Se você já mapeou usuários do S3 para usuários do nas e grupos criados, você pode configurar suas permissões e clique em **Salvar**. Você já deve ter mapeado S3 usuários para usuários nas antes de configurar permissões nesta etapa.

Caso contrário, clique em **Save** para concluir a configuração do bucket do nas do S3.

CLI

Crie um bucket do nas S3 em um SVM que contenha sistemas de arquivos nas. E
`vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-type nas -nas-path` *`junction_path`* `[-comment` *`text`*`]`

Exemplo
```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /vol1
```

Ative S3 usuários de cliente

Para permitir que os usuários de cliente S3 acessem dados nas, você deve mapear nomes de usuário S3 para os usuários nas correspondentes e conceder permissão para acessar os dados nas usando políticas de serviço de bucket.

Antes de começar

Os nomes de usuário para acesso ao cliente – usuários clientes LINUX/UNIX, Windows e S3 – já devem existir.

Você deve estar ciente de que alguma funcionalidade do S3 é "Não compatível com buckets do nas S3".

Sobre esta tarefa

Mapear um nome de usuário S3 para um USUÁRIO LINUX/UNIX ou Windows correspondente permite que verificações de autorização nos arquivos nas sejam honradas quando esses arquivos são acessados por clientes S3. Os mapeamentos S3 para nas são especificados fornecendo um nome de usuário S3 *pattern*, que pode ser expresso como um único nome ou uma expressão regular POSIX, e um nome de usuário

LINUX/UNIX ou Windows *Replacement*.

Caso não haja nenhum mapeamento de nomes presente, será usado o mapeamento de nomes padrão, onde o próprio nome de usuário S3 será usado como o nome de usuário UNIX e o nome de usuário do Windows. Você pode modificar os mapeamentos de nome de usuário padrão UNIX e Windows com o `vserver object-store-server modify` comando.

Apenas a configuração de mapeamento de nomes local é suportada; o LDAP não é suportado.

Depois que os usuários do S3 são mapeados para usuários nas, você pode conceder permissões aos usuários especificando os recursos (diretórios e arquivos) aos quais eles têm acesso e as ações que eles têm permissão ou não podem executar lá.

System Manager

1. Crie mapeamentos de nomes locais para clientes UNIX ou Windows (ou ambos).
   a. Clique em **Storage > Buckets** (armazenamento > baldes*) e selecione a VM de armazenamento habilitada para S3/nas.
   b. Selecione **Configurações** e clique → em **Mapeamento de nomes** (em **usuários e grupos de hosts**).
   c. Nos blocos **S3 para Windows** ou **S3 para UNIX** (ou ambos), clique em **Add** e, em seguida, insira os nomes de usuário **Pattern** (S3) e **Replacement** (nas) desejados.
2. Crie uma política de bucket para fornecer acesso ao cliente.
   a. Clique em **armazenamento > baldes**, clique ⋮ em junto ao balde S3 pretendido e, em seguida, clique em **Editar**.
   b. Clique em **Add** e forneça os valores desejados.
      - **Principal** - forneça S3 nomes de usuário ou use o padrão (todos os usuários).
      - **Efeito** - Selecione **permitir** ou **Negar**.
      - **Ações** - Digite as ações para esses usuários e recursos. O conjunto de operações de recursos que o servidor de armazenamento de objetos suporta atualmente para buckets do nas S3 são: GetObject, PutObject, DeletObject, ListBucketAcl, GetObjectTagging, PutObjectTagging, DeletObjectTagging, GetBucketLocation, GetBucketVerketversioning, PutBucketVerketverversions e ListBucketsions. Wildcards são aceitos para este parâmetro.
      - **Resources** - Insira caminhos de pasta ou arquivo nos quais as ações são permitidas ou negadas, ou use os padrões (diretório raiz do bucket).

CLI

1. Crie mapeamentos de nomes locais para clientes UNIX ou Windows (ou ambos). E `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - número de prioridade para a avaliação do mapeamento; introduza 1 ou 2.
   - `-pattern` - Um nome de usuário S3 ou uma expressão regular
   - `-replacement` - um nome de usuário do windows ou unix

Exemplos

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Crie uma política de bucket para fornecer acesso ao cliente. E `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - especifica se o acesso é permitido ou negado quando um usuário solicita uma ação.
   - `-action <Action>, …` - especifica operações de recursos que são permitidas ou negadas. O conjunto de operações de recursos que o servidor de armazenamento de objetos suporta atualmente para buckets do nas S3 são: GetObject, PutObject, DeleteObject, ListBucket,

GetBucketAcl, GetObjectAcl e GetBucketLocation. Wildcards são aceitos para este parâmetro.

- `-principal <Objectstore Principal>, …` - valida o usuário que solicita acesso aos usuários ou grupos de servidores de armazenamento de objetos especificados neste parâmetro.
  - Um grupo de servidores de armazenamento de objetos é especificado adicionando um grupo de prefixo/ ao nome do grupo.
  - `-principal` - (o caractere hífen) concede acesso a todos os usuários.
- `-resource <text>, …` - especifica o bucket, pasta ou objeto para o qual permissões de permissão/negação são definidas. Wildcards são aceitos para este parâmetro.
- `[-sid <SID>]` - especifica um comentário de texto opcional para a declaração de política de bucket do servidor de armazenamento de objetos.

Exemplos

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configuração SMB para Microsoft Hyper-V e SQL Server

Descrição geral da configuração SMB para Microsoft Hyper-V e SQL Server

Os recursos do ONTAP permitem que você ative operações ininterruptas para duas aplicações Microsoft através do protocolo SMB: Microsoft Hyper-V e Microsoft SQL Server.

Use esses procedimentos se quiser implementar operações ininterruptas SMB nas seguintes circunstâncias:

- O acesso básico ao ficheiro de protocolo SMB foi configurado.
- Você deseja habilitar compartilhamentos de arquivo SMB 3,0 ou posteriores residentes em SVMs para armazenar os seguintes objetos:
  - Arquivos de máquina virtual Hyper-V.
  - Bancos de dados do sistema do SQL Server

Informações relacionadas

Para obter informações adicionais sobre a tecnologia ONTAP e a interação com serviços externos, consulte estes relatórios técnicos (TRs): "Relatório técnico da NetApp 4172: Microsoft Hyper-V sobre SMB 3,0 com práticas recomendadas da ONTAP" ** "Relatório técnico do NetApp 4369: Práticas recomendadas para Microsoft SQL Server e SnapManager 7,2 para SQL Server com Clustered Data ONTAP"

Configure o ONTAP para as soluções Microsoft Hyper-V e SQL Server em SMB

Você pode usar compartilhamentos de arquivos SMB 3,0 e posteriores disponíveis

continuamente para armazenar arquivos de máquina virtual Hyper-V ou bancos de dados de sistema SQL Server e bancos de dados de usuários em volumes residentes em SVMs, ao mesmo tempo em que fornece operações ininterruptas (NDOs) para eventos planejados e não planejados.

Microsoft Hyper-V sobre SMB

Para criar uma solução Hyper-V sobre SMB, primeiro você deve configurar o ONTAP para fornecer serviços de armazenamento para servidores Microsoft Hyper-V. Além disso, você também deve configurar clusters da Microsoft (se estiver usando uma configuração em cluster), servidores Hyper-V, conexões SMB 3,0 continuamente disponíveis para os compartilhamentos hospedados pelo servidor CIFS e, opcionalmente, serviços de backup para proteger os arquivos de máquina virtual armazenados em volumes SVM.

> Os servidores Hyper-V devem ser configurados no Windows 2012 Server ou posterior. As configurações de servidor Hyper-V independentes e em cluster são suportadas.

- Para obter informações sobre como criar clusters da Microsoft e servidores Hyper-V, consulte o site da Microsoft.
- O SnapManager para Hyper-V é uma aplicação baseada em host que facilita os serviços de backup rápidos baseados em cópia Snapshot, projetados para se integrar às configurações do Hyper-V em SMB.

  Para obter informações sobre como usar o SnapManager com Hyper-V em configurações SMB, consulte *SnapManager para Guia de Instalação e Administração do Hyper-V*.

Microsoft SQL Server sobre SMB

Para criar uma solução SQL Server sobre SMB, primeiro você deve configurar o ONTAP para fornecer serviços de storage para a aplicação Microsoft SQL Server. Além disso, você também deve configurar clusters da Microsoft (se estiver usando uma configuração em cluster). Em seguida, você instalaria e configuraria o SQL Server nos servidores Windows e criaria conexões SMB 3,0 continuamente disponíveis para os compartilhamentos hospedados pelo servidor CIFS. Opcionalmente, você pode configurar serviços de backup para proteger os arquivos de banco de dados armazenados em volumes SVM.

> O SQL Server deve ser instalado e configurado no Windows 2012 Server ou posterior. Configurações autônomas e em cluster são compatíveis.

- Para obter informações sobre como criar clusters da Microsoft e instalar e configurar o SQL Server, consulte o site da Microsoft.
- O plug-in do SnapCenter para Microsoft SQL Server é uma aplicação baseada em host que facilita serviços de backup rápidos e baseados em cópias snapshot, projetados para serem integrados a configurações do SQL Server em SMB.

  Para obter informações sobre como usar o plug-in do SnapCenter para Microsoft SQL Server, consulte o "Plug-in do SnapCenter para Microsoft SQL Server" documento.

Operações ininterruptas para Hyper-V e SQL Server em SMB

O que significam operações ininterruptas para Hyper-V e SQL Server em SMB

Operações ininterruptas para Hyper-V e SQL Server sobre SMB referem-se à

combinação de funcionalidades que permitem que os servidores de aplicações e as máquinas virtuais ou bancos de dados contidos permaneçam on-line e forneçam disponibilidade contínua durante muitas tarefas administrativas. Isso inclui tempo de inatividade planejado e não planejado da infraestrutura de storage.

Operações ininterruptas compatíveis para servidores de aplicações em SMB incluem o seguinte:

- Takeover planejado e giveback
- Takeover não planejado
- Atualização
- Realocação de agregados planejada (ARL)
- Migração de LIF e failover
- Movimentação de volume planejada

Protocolos que permitem operações ininterruptas em SMB

Juntamente com o lançamento do SMB 3,0, a Microsoft lançou novos protocolos para fornecer os recursos necessários para dar suporte a operações ininterruptas para Hyper-V e SQL Server sobre SMB.

A ONTAP usa esses protocolos ao fornecer operações ininterruptas para servidores de aplicações em SMB:

- SMB 3,0
- Testemunha

Conceitos-chave sobre operações ininterruptas para Hyper-V e SQL Server sobre SMB

Há certos conceitos sobre operações ininterruptas (NDOs) que você deve entender antes de configurar sua solução Hyper-V ou SQL Server sobre SMB.

- **Partilha continuamente disponível**

  Um compartilhamento SMB 3,0 que tem o conjunto de propriedades de compartilhamento continuamente disponível. Os clientes que se conetam por meio de compartilhamentos disponíveis continuamente podem sobreviver a eventos disruptivos, como aquisição, giveback e realocação agregada.

- **Nó**

  Um único controlador que é membro de um cluster. Para distinguir entre os dois nós em um par de SFO, um nó é às vezes chamado de *nó local* e o outro nó é às vezes chamado de *nó parceiro* ou *nó remoto*. O principal proprietário do storage é o nó local. O proprietário secundário, que controla o storage quando o proprietário principal falha, é o nó do parceiro. Cada nó é o principal proprietário do storage e o proprietário secundário do storage do parceiro.

- * Realocação de agregados sem interrupções*

  Capacidade de mover um agregado entre nós de parceiros dentro de um par de SFO em um cluster sem interromper as aplicações de clientes.

- **Failover sem interrupções**

Veja *Takeover*.

- **Migração de LIF sem interrupções**

  A capacidade de realizar uma migração de LIF sem interromper aplicativos clientes conectados ao cluster por meio desse LIF. Para conexões SMB, isso só é possível para clientes que se conetam usando SMB 2,0 ou posterior.

- **Operações ininterruptas**

  Capacidade de executar grandes operações de gerenciamento e atualização do ONTAP, bem como resistir a falhas de nós sem interromper as aplicações dos clientes. Esse termo se refere à coleção de funcionalidades de aquisição sem interrupções, atualização sem interrupções e migração sem interrupções como um todo.

- **Atualização sem interrupções**

  Capacidade de atualizar o hardware ou o software do nó sem interrupção da aplicação.

- * Movimento de volume sem interrupções*

  Capacidade de mover um volume livremente pelo cluster sem interromper as aplicações que estão usando o volume. Para conexões SMB, todas as versões do SMB são compatíveis com movimentos de volume sem interrupções.

- * Alças persistentes*

  Uma propriedade do SMB 3,0 que permite que conexões continuamente disponíveis se reconetem de forma transparente ao servidor CIFS em caso de desconexão. Semelhante aos manipuladores duráveis, os manipuladores persistentes são mantidos pelo servidor CIFS por um período de tempo após a perda da comunicação com o cliente de conexão. No entanto, alças persistentes têm mais resiliência do que alças duráveis. Além de dar ao cliente a chance de recuperar o identificador dentro de uma janela de 60 segundos após a reconexão, o servidor CIFS nega acesso a quaisquer outros clientes que solicitem acesso ao arquivo durante essa janela de 60 segundos.

  As informações sobre alças persistentes são espelhadas no armazenamento persistente do parceiro SFO, o que permite que os clientes com alças persistentes desconetadas recuperem as alças duráveis após um evento em que o parceiro SFO assuma a propriedade do armazenamento do nó. Além de fornecer operações ininterruptas no caso de mudanças de LIF (que são duráveis lidar com o suporte), as alças persistentes fornecem operações ininterruptas para takeover, giveback e realocação de agregados.

- **SFO**

  Retorno de agregados para seus locais de origem ao se recuperar de um evento de aquisição.

- **Par SFO**

  Um par de nós cujos controladores estão configurados para servir dados entre si se um dos dois nós deixar de funcionar. Dependendo do modelo do sistema, ambos os controladores podem estar em um único chassi ou os controladores podem estar em um chassi separado. Conhecido como um par de HA em um cluster de dois nós.

- **Aquisição**

  O processo pelo qual o parceiro assume o controle do storage quando o proprietário principal desse storage falha. No contexto de SFO, failover e aquisição são sinônimos.

Como a funcionalidade SMB 3,0 dá suporte a operações ininterruptas por compartilhamentos SMB

O SMB 3,0 fornece funcionalidade crucial que permite o suporte a operações ininterruptas para compartilhamentos Hyper-V e SQL Server em SMB. Isso inclui a `continuously-available` propriedade compartilhar e um tipo de identificador de arquivo conhecido como *identificador persistente* que permite que os clientes SMB recuperem o estado aberto do arquivo e restabeleçam conexões SMB de forma transparente.

Identificadores persistentes podem ser concedidos a clientes compatíveis com SMB 3,0 que se conetam a um compartilhamento com o conjunto de propriedades de compartilhamento continuamente disponível. Se a sessão SMB for desconetada, o servidor CIFS retém informações sobre o estado de identificador persistente. O servidor CIFS bloqueia outras solicitações de cliente durante o período de 60 segundos em que o cliente pode se reconetar, permitindo assim que o cliente com o identificador persistente recupere o identificador após uma desconexão da rede. Os clientes com alças persistentes podem se reconetar usando uma das LIFs de dados na máquina virtual de storage (SVM), seja reconetando pelo mesmo LIF ou por meio de um LIF diferente.

A realocação agregada, a aquisição e a giveback ocorrem entre pares de SFO. Para gerenciar de forma otimizada a desconexão e a reconexão de sessões com arquivos com alças persistentes, o nó do parceiro mantém uma cópia de todas as informações de bloqueio de identificador persistente. Independentemente de o evento ser planejado ou não planejado, o parceiro SFO pode gerenciar as reconexões de identificador persistente sem interrupções. Com essa nova funcionalidade, as conexões SMB 3,0 ao servidor CIFS podem fazer failover de forma transparente e sem interrupções para outro LIF de dados atribuído à SVM em eventos que tradicionalmente têm sido disruptivos.

Embora o uso de alças persistentes permita que o servidor CIFS faça failover transparente em conexões SMB 3,0, se uma falha fizer com que o aplicativo Hyper-V faça failover para outro nó no cluster do Windows Server, o cliente não terá como recuperar as alças de arquivo dessas alças desconetadas. Nesse cenário, os manipuladores de arquivos no estado desconetado podem potencialmente bloquear o acesso do aplicativo Hyper-V se ele for reiniciado em um nó diferente. "'Cluster de failover'" é uma parte do SMB 3,0 que aborda esse cenário fornecendo um mecanismo para invalidar manipulações obsoletas e conflitantes. Usando esse mecanismo, um cluster Hyper-V pode se recuperar rapidamente quando os nós de cluster Hyper-V falham.

O que o protocolo Witness faz para melhorar o failover transparente

O protocolo Witness fornece recursos aprimorados de failover de cliente para compartilhamentos continuamente disponíveis (compartilhamentos CA) SMB 3,0. O Witness facilita o failover mais rápido porque ignora o período de recuperação de failover de LIF. Ele notifica os servidores de aplicativos quando um nó não está disponível sem a necessidade de esperar que a conexão SMB 3,0 expire.

O failover é contínuo, com as aplicações em execução no cliente não cientes de que ocorreu um failover. Se a testemunha não estiver disponível, as operações de failover ainda ocorrem com sucesso, mas o failover sem testemunha é menos eficiente.

O failover aprimorado de testemunhas é possível quando os seguintes requisitos são atendidos:

- Ele só pode ser usado com servidores CIFS compatíveis com SMB 3,0 que tenham SMB 3,0 habilitado.
- Os compartilhamentos devem usar o SMB 3,0 com o conjunto de propriedades de compartilhamento de disponibilidade contínua.

- O parceiro SFO do nó ao qual os servidores de aplicativos estão conetados deve ter pelo menos um LIF de dados operacional atribuído à máquina virtual de armazenamento (SVM) que hospeda dados para os servidores de aplicativos.

> O protocolo testemunha opera entre pares SFO. Como os LIFs podem migrar para qualquer nó dentro do cluster, qualquer nó pode precisar ser a testemunha de seu parceiro SFO. O protocolo Witness não pode fornecer failover rápido de conexões SMB em um determinado nó se os dados de hospedagem SVM para os servidores de aplicações não tiverem um LIF de dados ativo no nó de parceiro. Portanto, cada nó no cluster precisa ter pelo menos um data LIF para cada SVM que hospeda uma dessas configurações.

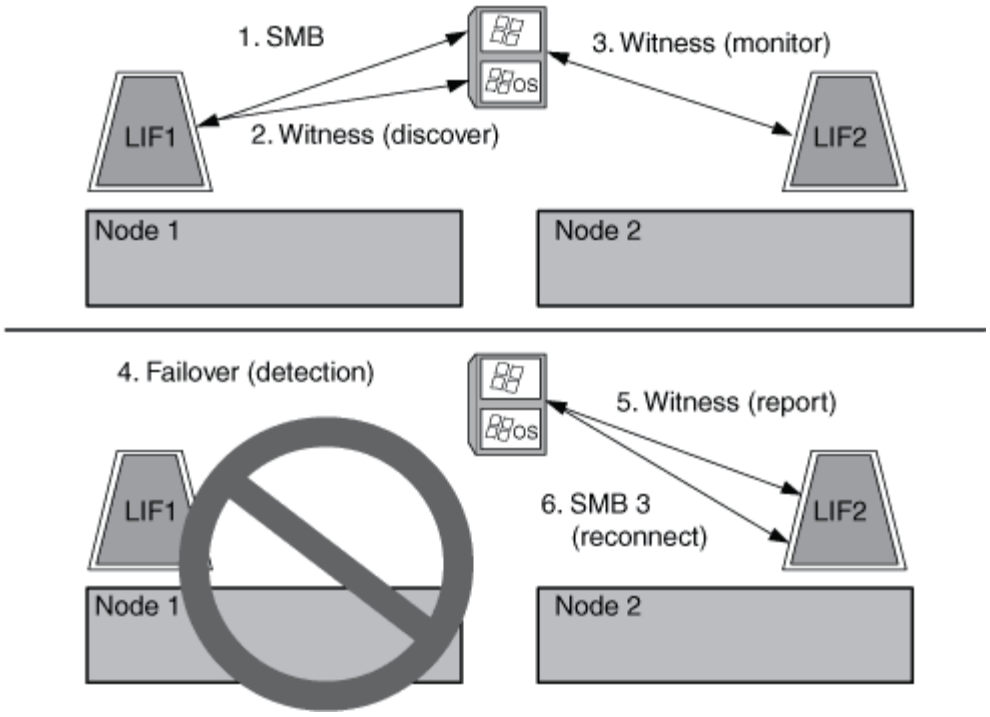
- Os servidores de aplicativos devem se conetar ao servidor CIFS usando o nome do servidor CIFS que é armazenado no DNS em vez de usando endereços IP de LIF individuais.

Como funciona o protocolo testemunha

O ONTAP implementa o protocolo Witness usando o parceiro SFO de um nó como testemunha. Em caso de falha, o parceiro deteta rapidamente a falha e notifica o cliente SMB.

O protocolo Witness fornece failover aprimorado usando o seguinte processo:

1. Quando o servidor de aplicativos estabelece uma conexão SMB continuamente disponível ao Node1, o servidor CIFS informa ao servidor de aplicativos que a testemunha está disponível.
2. O servidor do aplicativo solicita os endereços IP do servidor testemunha de Node1 e recebe uma lista de Node2 (o parceiro SFO) endereços IP de LIF de dados atribuídos à máquina virtual de armazenamento (SVM).
3. O servidor de aplicativos escolhe um dos endereços IP, cria uma conexão testemunha com o Node2 e se Registra para ser notificado se a conexão continuamente disponível no Node1 precisar se mover.
4. Se um evento de failover ocorrer no Node1, o Witness facilita os eventos de failover, mas não está envolvido com a giveback.
5. O Witness deteta o evento de failover e notifica o servidor de aplicativos por meio da conexão Witness que a conexão SMB deve ser movida para Node2.
6. O servidor de aplicativos move a sessão SMB para Node2 e recupera a conexão sem interrupção ao acesso do cliente.



Backups baseados em compartilhamento com VSS remoto

Backups baseados em compartilhamento com a visão geral do VSS remoto

Você pode usar o VSS remoto para executar backups baseados em compartilhamento de arquivos de máquina virtual Hyper-V armazenados em um servidor CIFS.

Microsoft Remote VSS (volume Shadow Copy Services) é uma extensão da infraestrutura Microsoft VSS existente. Com o VSS remoto, a Microsoft estendeu a infraestrutura VSS para dar suporte à cópia sombra de compartilhamentos SMB. Além disso, aplicativos de servidor, como o Hyper-V, podem armazenar arquivos VHD em compartilhamentos de arquivos SMB. Com essas extensões, é possível fazer cópias de sombra consistentes de aplicativos para máquinas virtuais que armazenam dados e arquivos de configuração em compartilhamentos.

Conceitos VSS remotos

Você deve estar ciente de certos conceitos que são necessários para entender como o VSS remoto (volume Shadow Copy Service) é usado por serviços de backup com configurações Hyper-V em SMB.

- **VSS (Serviço de cópia sombra de volume)**

  Uma tecnologia da Microsoft usada para fazer cópias de backup ou snapshots de dados em um volume específico em um determinado momento. O VSS coordena entre servidores de dados, aplicações de backup e software de gerenciamento de storage para dar suporte à criação e gerenciamento de backups consistentes.

- * VSS remoto (Serviço de cópia de sombra de volume remoto)*

  Uma tecnologia da Microsoft usada para fazer cópias de backup baseadas em compartilhamento de dados que estão em um estado consistente com dados em um momento específico em que os dados são acessados por compartilhamentos SMB 3,0. Também conhecido como *volume Shadow Copy Service*.

- **Cópia sombra**

  Um conjunto duplicado de dados contidos no compartilhamento em um instante bem definido no tempo. As cópias de sombra são usadas para criar backups consistentes de dados pontuais, permitindo que o sistema ou as aplicações continuem atualizando os dados nos volumes originais.

- * Conjunto de cópias de sombra*

  Uma coleção de uma ou mais cópias de sombra, com cada cópia de sombra correspondente a um compartilhamento. As cópias de sombra dentro de um conjunto de cópias de sombra representam todos os compartilhamentos que precisam ser copiados na mesma operação. O cliente VSS no aplicativo habilitado para VSS identifica quais cópias de sombra incluir no conjunto.

- * Recuperação automática do conjunto de cópias sombra*

  A parte do processo de backup para aplicativos de backup remotos habilitados para VSS, em que o diretório de réplica que contém as cópias sombra é consistente ponto no tempo. No início do backup, o cliente VSS no aplicativo aciona o aplicativo para fazer pontos de verificação de software sobre os dados programados para backup (os arquivos de máquina virtual no caso do Hyper-V). Em seguida, o cliente VSS permite que os aplicativos continuem. Depois que o conjunto de cópias de sombra é criado, o VSS remoto torna o conjunto de cópias de sombra gravável e expõe a cópia gravável para os aplicativos. O aplicativo prepara o conjunto de cópias de sombra para backup executando uma recuperação automática usando o ponto de verificação de software feito anteriormente. A recuperação automática traz as cópias de sombra para um estado consistente, desrolando as alterações feitas nos arquivos e diretórios desde que o ponto de verificação foi criado. A recuperação automática é uma etapa opcional para backups habilitados para VSS.

- **ID de cópia sombra**

  Um GUID que identifica exclusivamente uma cópia de sombra.

- **ID do conjunto de cópias sombra**

  Um GUID que identifica exclusivamente uma coleção de IDs de cópia de sombra para o mesmo servidor.

- **SnapManager para Hyper-V**

  O software que automatiza e simplifica as operações de backup e restauração para o Microsoft Windows Server 2012 Hyper-V. o SnapManager para Hyper-V usa o VSS remoto com recuperação automática para fazer backup de arquivos Hyper-V em compartilhamentos SMB.

Informações relacionadas

Conceitos-chave sobre operações ininterruptas para Hyper-V e SQL Server sobre SMB

Backups baseados em compartilhamento com VSS remoto

Exemplo de uma estrutura de diretório usada pelo VSS remoto

O VSS remoto percorre a estrutura de diretórios que armazena arquivos de máquina virtual Hyper-V enquanto cria cópias de sombra. É importante entender o que é uma estrutura de diretório apropriada, para que você possa criar com sucesso backups de arquivos de máquina virtual.

Uma estrutura de diretório suportada para a criação bem-sucedida de cópias sombra está em conformidade

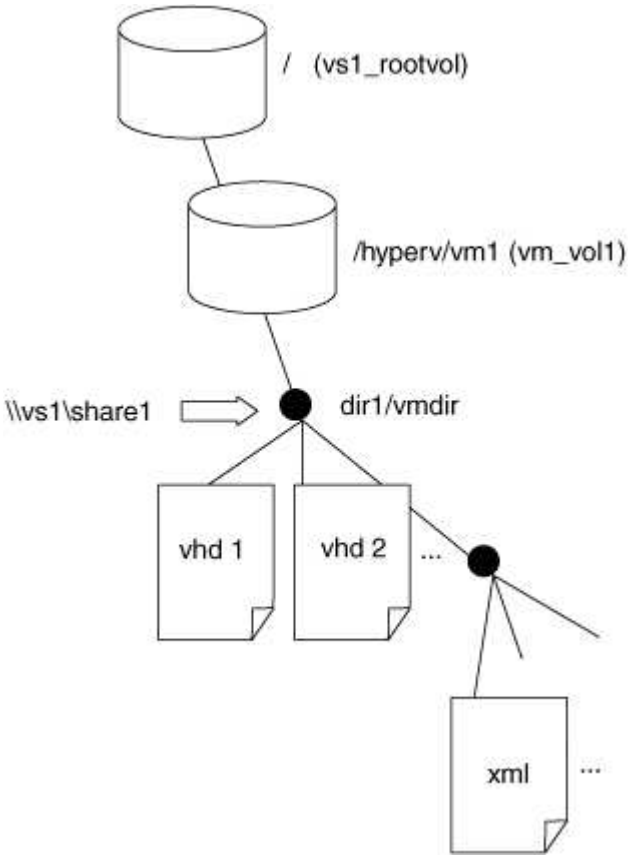
com os seguintes requisitos:

- Somente diretórios e arquivos regulares estão presentes dentro da estrutura de diretórios que é usada para armazenar arquivos de máquina virtual.

  A estrutura de diretórios não contém junções, links ou arquivos não regulares.

- Todos os arquivos de uma máquina virtual residem em um único compartilhamento.
- A estrutura de diretórios que é usada para armazenar arquivos de máquina virtual não excede a profundidade configurada do diretório de cópia de sombra.
- O diretório raiz do compartilhamento contém apenas arquivos ou diretórios de máquina virtual.

Na ilustração a seguir, o volume chamado VM_vol1 é criado com um ponto de junção em `/hyperv/vm1` na máquina virtual de armazenamento (SVM) VS1. Subdiretórios para conter os arquivos da máquina virtual são criados sob o ponto de junção. Os arquivos de máquina virtual do servidor Hyper-V são acessados em share1 que tem o `/hyperv/vm1/dir1/vmdir` caminho . O serviço de cópia de sombra cria cópias de sombra de todos os arquivos de máquina virtual que estão contidos na estrutura de diretórios sob share1 (até a profundidade configurada do diretório de cópia de sombra).



Como o SnapManager para Hyper-V gerencia backups remotos baseados em VSS para Hyper-V em SMB

Você pode usar o SnapManager para Hyper-V para gerenciar serviços de backup baseados em VSS remoto. Há benefícios de usar o serviço de backup gerenciado do SnapManager para Hyper-V para criar conjuntos de backup com uso eficiente de espaço.

As otimizações para o SnapManager para backups gerenciados do Hyper-V incluem o seguinte:

- A integração do SnapDrive com o ONTAP oferece otimização de performance ao descobrir o local de compartilhamento SMB.

  O ONTAP fornece ao SnapDrive o nome do volume em que o compartilhamento reside.

- O SnapManager para Hyper-V especifica a lista de arquivos de máquina virtual nos compartilhamentos SMB que o serviço de cópia sombra precisa copiar.

  Ao fornecer uma lista segmentada de arquivos de máquina virtual, o serviço de cópia de sombra não precisa criar cópias de sombra de todos os arquivos no compartilhamento.

- A máquina virtual de storage (SVM) retém as cópias Snapshot do SnapManager para Hyper-V a serem usadas para restaurações.

  Não há fase de backup. O backup é a cópia Snapshot com uso eficiente de espaço.

O SnapManager para Hyper-V fornece recursos de backup e restauração para o HyperV em SMB usando o seguinte processo:

1. Preparação para a operação de cópia de sombra

   O cliente VSS do aplicativo SnapManager para Hyper-V configura o conjunto de cópias de sombra. O cliente VSS reúne informações sobre quais compartilhamentos incluir no conjunto de cópias de sombra e fornece essas informações ao ONTAP. Um conjunto pode conter uma ou mais cópias de sombra, e uma cópia de sombra corresponde a um compartilhamento.

2. Criando o conjunto de cópias de sombra (se a recuperação automática for usada)

   Para cada compartilhamento incluído no conjunto de cópias de sombra, o ONTAP cria uma cópia de sombra e torna a cópia de sombra gravável.

3. Expondo o conjunto de cópias de sombra

   Depois que o ONTAP cria as cópias de sombra, elas são expostas ao SnapManager para Hyper-V para que os escritores VSS do aplicativo possam executar a recuperação automática.

4. Recuperar automaticamente o conjunto de cópias de sombra

   Durante a criação do conjunto de cópias de sombra, há um período de tempo em que as alterações ativas estão ocorrendo nos arquivos incluídos no conjunto de backup. Os escritores VSS do aplicativo devem atualizar as cópias sombra para garantir que estejam em um estado completamente consistente antes do backup.

   > A forma como a recuperação automática é feita é específica da aplicação. VSS remoto não está envolvido nesta fase.

5. Completar e limpar o conjunto de cópias de sombra

   O cliente VSS notifica o ONTAP após concluir a recuperação automática. O conjunto de cópias de sombra é feito somente leitura e, em seguida, está pronto para backup. Ao usar o SnapManager para Hyper-V para backup, os arquivos em uma cópia Snapshot tornam-se o backup; portanto, para a fase de backup, uma cópia Snapshot é criada para cada volume que contém compartilhamentos no conjunto de backup. Após a conclusão do backup, o conjunto de cópias de sombra é removido do servidor CIFS.

Como a descarga de cópia ODX é usada com Hyper-V e SQL Server em compartilhamentos SMB

A transferência de dados descarregados (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host. A descarga de cópia ODX da ONTAP fornece benefícios de desempenho ao executar operações de cópia no servidor de aplicações através da instalação SMB.

Em transferências de arquivos não ODX, os dados são lidos do servidor CIFS de origem e são transferidos através da rede para o computador cliente. O computador cliente transfere os dados de volta pela rede para o servidor CIFS de destino. Em resumo, o computador cliente lê os dados da origem e grava-os no destino. Com as transferências de arquivos ODX, os dados são copiados diretamente da origem para o destino.

Como as cópias descarregadas do ODX são realizadas diretamente entre o armazenamento de origem e destino, há benefícios significativos de desempenho. Os benefícios de desempenho obtidos incluem tempo de cópia mais rápido entre a origem e o destino, utilização reduzida de recursos (CPU, memória) no cliente e utilização reduzida da largura de banda de e/S de rede.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:
```

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e mesma máquina virtual de storage (SVM)

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

Casos de uso específicos para descarga de cópia ODX com soluções Hyper-V incluem o seguinte:

- Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

> Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Casos de uso específicos para descarga de cópia ODX com soluções SQL Server incluem o seguinte:

- Você pode usar a descarga de cópia ODX para exportar e importar bancos de dados SQL Server entre compartilhamentos SMB mapeados ou entre compartilhamentos SMB e LUNs iSCSI conetados no mesmo cluster.
- A descarga de cópia ODX é usada para exportações e importações de banco de dados se o armazenamento de origem e destino estiver no mesmo cluster.

Requisitos e considerações de configuração

Requisitos de ONTAP e licenciamento

Você precisa estar ciente de certos requisitos de licenciamento e ONTAP ao criar soluções SQL Server ou Hyper-V em SMB para operações ininterruptas em SVMs.

Requisitos de versão do ONTAP

- Hyper-V em SMB

  O ONTAP é compatível com operações ininterruptas por compartilhamentos SMB para Hyper-V executados no Windows 2012 ou posterior.

- SQL Server sobre SMB

  O ONTAP é compatível com operações ininterruptas por compartilhamentos SMB para SQL Server 2012 ou posterior executados no Windows 2012 ou posterior.

Para obter as informações mais recentes sobre versões com suporte do ONTAP, Windows Server e SQL Server para operações ininterruptas em compartilhamentos SMB, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos de licenciamento

São necessárias as seguintes licenças:

- CIFS
- FlexClone (somente para Hyper-V em SMB)

  Esta licença é necessária se o VSS remoto for usado para backups. O serviço de cópia de sombra usa o

FlexClone para criar cópias pontuais de arquivos que são então usados ao criar um backup.

Uma licença do FlexClone é opcional se você usar um método de backup que não use o VSS remoto.

A licença FlexClone está incluída no "ONTAP One". Se não tiver o ONTAP One, deverá "verifique se as licenças necessárias estão instaladas", e, se necessário"instale-os", .

Requisitos de LIF de rede e dados

Você precisa estar ciente de certos requisitos de rede e de LIF de dados ao criar configurações do SQL Server ou Hyper-V em SMB para operações ininterruptas).

Requisitos de protocolo de rede

- São suportadas redes IPv4G e IPv6G.
- SMB 3,0 ou posterior é necessário.

  O SMB 3,0 fornece a funcionalidade necessária para criar as conexões SMB continuamente disponíveis necessárias para oferecer operações ininterruptas.

- Os servidores DNS devem conter entradas que mapeiam o nome do servidor CIFS para os endereços IP atribuídos aos LIFs de dados na máquina virtual de armazenamento (SVM).

  Os servidores de aplicativos Hyper-V ou SQL Server normalmente fazem várias conexões em várias LIFs de dados ao acessar arquivos de máquina virtual ou banco de dados. Para uma funcionalidade adequada, os servidores de aplicativos devem fazer essas várias conexões SMB usando o nome do servidor CIFS em vez de fazer várias conexões com vários endereços IP exclusivos.

  Witness também requer o uso do nome DNS do servidor CIFS em vez de endereços IP LIF individuais.

  A partir do ONTAP 9.4, você pode melhorar a taxa de transferência e a tolerância a falhas para as configurações Hyper-V e SQL Server em SMB, ativando o Multichannel SMB. Para fazer isso, você deve ter várias NICs de 1G, 10G ou maiores implantados no cluster e nos clientes.

Requisitos de LIF de dados

- O SVM que hospeda a solução de servidor de aplicações em SMB precisa ter pelo menos um LIF de dados operacionais em cada nó do cluster.

  Os LIFs de dados do SVM podem fazer failover para outras portas de dados no cluster, incluindo nós que não estão hospedando dados acessados pelos servidores de aplicações. Além disso, como o nó testemunha é sempre o parceiro SFO de um nó ao qual o servidor de aplicativos está conetado, cada nó no cluster é um nó de testemunha potencial.

- Os LIFs de dados não devem ser configurados para reverter automaticamente.

  Após um evento de aquisição ou giveback, você deve reverter manualmente os LIFs de dados para suas portas domésticas.

- Todos os endereços IP de LIF de dados devem ter uma entrada no DNS e todas as entradas devem ser resolvidas para o nome do servidor CIFS.

  Os servidores de aplicativos devem se conetar a compartilhamentos SMB usando o nome do servidor CIFS. Você não deve configurar os servidores de aplicativos para fazer conexões usando os endereços IP

LIF.

- Se o nome do servidor CIFS for diferente do nome SVM, as entradas DNS deverão ser resolvidas para o nome do servidor CIFS.

Requisitos de volume e servidor SMB para Hyper-V em SMB

Você precisa estar ciente de certos requisitos de volume e servidor SMB ao criar configurações Hyper-V em SMB para operações ininterruptas.

Requisitos de servidor SMB

- O SMB 3,0 deve estar ativado.

  Esta opção está ativada por predefinição.

- A opção de servidor CIFS de usuário UNIX padrão deve ser configurada com uma conta de usuário UNIX válida.

  Os servidores de aplicativos usam a conta de máquina ao criar uma conexão SMB. Como todo o acesso SMB requer que o usuário do Windows mapeie com êxito para uma conta de usuário UNIX ou para a conta de usuário UNIX padrão, o ONTAP deve ser capaz de mapear a conta de máquina do servidor de aplicativos para a conta de usuário UNIX padrão.

- As referências de nó automáticas devem ser desativadas (esta funcionalidade está desativada por predefinição).

  Se você quiser usar referências de nó automáticas para acesso a dados que não sejam arquivos de máquina do Hyper-V, crie um SVM separado para esses dados.

- A autenticação Kerberos e NTLM devem ser permitidas no domínio ao qual o servidor SMB pertence.

  O ONTAP não anuncia o serviço Kerberos para VSS remoto; portanto, o domínio deve ser definido para permitir NTLM.

- A funcionalidade de cópia sombra deve estar ativada.

  Esta funcionalidade está ativada por predefinição.

- A conta de domínio do Windows que o serviço de cópia de sombra usa ao criar cópias de sombra deve ser membro do grupo de administradores locais do servidor SMB ou operadores de backup.

Requisitos de volume

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer NDOs para servidores de aplicativos usando conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Não é possível alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para NDOs em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para NDOs em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de

arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Para que as operações de cópia de sombra sejam bem-sucedidas, você precisa ter espaço disponível suficiente no volume.

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos de volume e servidor SMB para SQL Server em SMB

Você precisa estar ciente de certos requisitos de volume e servidor SMB ao criar configurações do SQL Server em SMB para operações ininterruptas.

Requisitos de servidor SMB

- O SMB 3,0 deve estar ativado.

  Esta opção está ativada por predefinição.

- A opção de servidor CIFS de usuário UNIX padrão deve ser configurada com uma conta de usuário UNIX válida.

  Os servidores de aplicativos usam a conta de máquina ao criar uma conexão SMB. Como todo o acesso SMB requer que o usuário do Windows mapeie com êxito para uma conta de usuário UNIX ou para a conta de usuário UNIX padrão, o ONTAP deve ser capaz de mapear a conta de máquina do servidor de aplicativos para a conta de usuário UNIX padrão.

  Além disso, o SQL Server usa um usuário de domínio como a conta de serviço do SQL Server. A conta de serviço também deve ser mapeada para o usuário UNIX padrão.

- As referências de nó automáticas devem ser desativadas (esta funcionalidade está desativada por predefinição).

  Se você quiser usar referências de nó automáticas para acesso a dados que não sejam arquivos de banco de dados do SQL Server, você deve criar um SVM separado para esses dados.

- A conta de usuário do Windows usada para instalar o SQL Server no ONTAP deve ser atribuída ao privilégio SeSecurityPrivilege.

  Este privilégio é atribuído ao grupo de administradores/BUILTIN local do servidor SMB.

Requisitos de volume

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer NDOs para servidores de aplicativos usando conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um

volume NTFS. Não é possível alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para NDOs em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para NDOs em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Embora o volume que contém os arquivos do banco de dados possa conter junções, o SQL Server não cruza junções ao criar a estrutura do diretório do banco de dados.
- Para que as operações de backup do SnapCenter Plug-in para Microsoft SQL Server sejam bem-sucedidas, você deve ter espaço disponível suficiente no volume.

  O volume no qual os arquivos de banco de dados do SQL Server residem deve ser grande o suficiente para manter a estrutura de diretório de banco de dados e todos os arquivos contidos dentro do compartilhamento.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos e considerações de compartilhamento continuamente disponíveis para Hyper-V sobre SMB

Você precisa estar ciente de certos requisitos e considerações ao configurar compartilhamentos disponíveis continuamente para configurações do Hyper-V em SMB que dão suporte a operações ininterruptas.

Compartilhar requisitos

- Os compartilhamentos usados pelos servidores de aplicativos devem ser configurados com o conjunto de propriedades continuamente disponível.

  Os servidores de aplicações que se conectam a compartilhamentos continuamente disponíveis recebem alças persistentes que lhes permitem se reconectarem sem interrupções aos compartilhamentos de SMB e recuperarem bloqueios de arquivos após eventos disruptivos, como takeover, giveback e realocação de agregados.

- Se você quiser usar serviços de backup habilitados para VSS remoto, não será possível colocar arquivos Hyper-V em compartilhamentos que contenham junções.

  No caso de recuperação automática, a criação de cópia sombra falha se uma junção for encontrada ao atravessar o compartilhamento. No caso não auto-recuperação, a criação de cópia sombra não falha, mas a junção não aponta para nada.

- Se você quiser usar serviços de backup habilitados para VSS remoto com recuperação automática, não será possível colocar arquivos Hyper-V em compartilhamentos que contenham o seguinte:
  - Links simbólicos, hardlinks ou widelinks
  - Arquivos não regulares

    A criação de cópia sombra falha se houver links ou arquivos não regulares na cópia compartilhar para sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

- Para que as operações de cópia sombra tenham sucesso, você deve ter espaço disponível suficiente no volume (somente para Hyper-V sobre SMB).

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

- As seguintes propriedades de compartilhamento não devem ser definidas em compartilhamentos continuamente disponíveis usados pelos servidores de aplicativos:
  - Diretório base
  - Armazenamento em cache de atributos
  - BranchCache

Considerações

- As cotas são suportadas em ações continuamente disponíveis.
- A seguinte funcionalidade não é suportada para configurações Hyper-V em SMB:
  - Auditoria
  - FPolicy
- A verificação de vírus não é realizada em compartilhamentos SMB com o `continuously-availability` parâmetro definido como `Yes`.

Requisitos e considerações de compartilhamento continuamente disponíveis para SQL Server sobre SMB

Você precisa estar ciente de certos requisitos e considerações ao configurar compartilhamentos continuamente disponíveis para configurações do SQL Server em SMB que dão suporte a operações ininterruptas.

Compartilhar requisitos

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer operações ininterruptas para servidores de aplicações que usam conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Você não pode alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para operações ininterruptas em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para operações ininterruptas em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Os compartilhamentos usados pelos servidores de aplicativos devem ser configurados com o conjunto de propriedades continuamente disponível.

  Os servidores de aplicações que se conectam a compartilhamentos continuamente disponíveis recebem

alças persistentes que lhes permitem se reconectarem sem interrupções aos compartilhamentos de SMB e recuperarem bloqueios de arquivos após eventos disruptivos, como takeover, giveback e realocação de agregados.

- Embora o volume que contém os arquivos do banco de dados possa conter junções, o SQL Server não cruza junções ao criar a estrutura do diretório do banco de dados.
- Para que o plug-in do SnapCenter para operações do Microsoft SQL Server seja bem-sucedido, você deve ter espaço disponível suficiente no volume.

  O volume no qual os arquivos de banco de dados do SQL Server residem deve ser grande o suficiente para manter a estrutura de diretório de banco de dados e todos os arquivos contidos dentro do compartilhamento.

- As seguintes propriedades de compartilhamento não devem ser definidas em compartilhamentos continuamente disponíveis usados pelos servidores de aplicativos:
  - Diretório base
  - Armazenamento em cache de atributos
  - BranchCache

Considerações sobre compartilhamento

- As cotas são suportadas em ações continuamente disponíveis.
- A seguinte funcionalidade não é suportada para configurações do SQL Server em SMB:
  - Auditoria
  - FPolicy
- A verificação de vírus não é realizada em compartilhamentos SMB com o `continuously-availability` conjunto de propriedades de compartilhamento.

Considerações sobre VSS remoto para configurações Hyper-V em SMB

Você precisa estar ciente de certas considerações ao usar soluções de backup habilitadas para VSS remotas para configurações Hyper-V sobre SMB.

Considerações gerais sobre o VSS remoto

- Um máximo de 64 compartilhamentos pode ser configurado por servidor de aplicativos da Microsoft.

  A operação de cópia de sombra falha se houver mais de 64 compartilhamentos em um conjunto de cópias de sombra. Este é um requisito da Microsoft.

- Apenas é permitido um conjunto de cópias de sombra ativo por servidor CIFS.

  Uma operação de cópia sombra falhará se houver uma operação de cópia sombra contínua no mesmo servidor CIFS. Este é um requisito da Microsoft.

- Nenhuma junção é permitida dentro da estrutura de diretórios na qual o VSS remoto cria uma cópia de sombra.
  - No caso de recuperação automática, a criação de cópia de sombra falhará se uma junção for encontrada ao atravessar o compartilhamento.
  - No caso de recuperação não automática, a criação de cópia sombra não falha, mas a junção não

aponta para nada.

Considerações do VSS remoto que se aplicam somente a cópias de sombra com recuperação automática

Certos limites se aplicam apenas a cópias sombra com recuperação automática.

- Uma profundidade máxima de diretório de cinco subdiretórios é permitida para a criação de cópias de sombra.

  Esta é a profundidade do diretório sobre a qual o serviço de cópia sombra cria um conjunto de backup de cópia sombra. A criação de cópia de sombra falhará se os diretórios que contêm arquivo de máquina virtual estiverem aninhados mais profundamente do que cinco níveis. Isto destina-se a limitar a travessia de diretório ao clonar o compartilhamento. A profundidade máxima do diretório pode ser alterada usando uma opção de servidor CIFS.

- A quantidade de espaço disponível no volume deve ser adequada.

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra.

- Não são permitidos links ou arquivos não regulares dentro da estrutura de diretórios na qual o VSS remoto cria uma cópia de sombra.

  A criação de cópia sombra falha se houver links ou arquivos não regulares no compartilhamento para a cópia sombra. O processo de clone não os suporta.

- Não são permitidas ACLs NFSv4 nos diretórios.

  Embora a criação de cópia sombra retenha NFSv4 ACLs em arquivos, as ACLs NFSv4 nos diretórios são perdidas.

- Um máximo de 60 segundos é permitido criar um conjunto de cópias de sombra.

  As especificações da Microsoft permitem um máximo de 60 segundos para criar o conjunto de cópias de sombra. Se o cliente VSS não puder criar o conjunto de cópias de sombra dentro desse tempo, a operação de cópia de sombra falhará; portanto, isso limita o número de arquivos em um conjunto de cópias de sombra. O número real de arquivos ou máquinas virtuais que podem ser incluídos em um conjunto de backup varia; esse número depende de muitos fatores e deve ser determinado para cada ambiente de cliente.

Requisitos de descarga de cópia ODX para SQL Server e Hyper-V sobre SMB

A descarga de cópia ODX deve ser ativada se você quiser migrar arquivos de máquina virtual ou exportar e importar arquivos de banco de dados diretamente da origem para o local de armazenamento de destino sem enviar dados através dos servidores de aplicativos. Há certos requisitos que você deve entender sobre o uso de descarga de cópia ODX com soluções SQL Server e Hyper-V sobre SMB.

O uso de descarga de cópia ODX proporciona um benefício significativo de desempenho. Esta opção de servidor CIFS está ativada por predefinição.

- O SMB 3,0 deve estar habilitado para usar a descarga de cópia ODX.

- Os volumes de origem devem ter no mínimo 1,25 GB.
- A deduplicação deve ser habilitada em volumes usados com descarga de cópia.
- Se você usar volumes compatados, o tipo de compactação deve ser adaptável e somente o tamanho do grupo de compactação 8K é suportado.

  O tipo de compressão secundária não é suportado

- Para usar a descarga de cópia ODX para migrar convidados Hyper-V dentro e entre discos, os servidores Hyper-V devem ser configurados para usar discos SCSI.

  O padrão é configurar discos IDE, mas a descarga de cópia ODX não funciona quando os convidados são migrados se os discos são criados usando discos IDE.

Recomendações para configurações do SQL Server e Hyper-V em SMB

Para ter certeza de que as configurações do SQL Server e do Hyper-V sobre SMB são robustas e operacionais, você precisa estar familiarizado com as práticas recomendadas ao configurar as soluções.

Recomendações gerais

- Separe os arquivos do servidor de aplicativos dos dados gerais do usuário.

  Se possível, dedique uma máquina virtual de storage inteira (SVM) e seu armazenamento aos dados do servidor de aplicativos.

- Para obter o melhor desempenho, não ative a assinatura SMB em SVMs que são usadas para armazenar os dados do servidor de aplicativos.
- Para melhor desempenho e melhor tolerância a falhas, ative o multicanal SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB.
- Não crie compartilhamentos continuamente disponíveis em compartilhamentos diferentes daqueles usados na configuração Hyper-V ou SQL Server sobre SMB.
- Desative o Change Notify em compartilhamentos usados para disponibilidade contínua.
- Não realize uma movimentação de volume ao mesmo tempo que o ARL (Aggregate Relocation) porque o ARL tem fases que pausam algumas operações.
- Para soluções Hyper-V sobre SMB, use unidades iSCSI convidadas ao criar máquinas virtuais em cluster. Os arquivos compartilhados `.VHDX` não são compatíveis com Hyper-V em SMB em compartilhamentos SMB do ONTAP.

Planeje a configuração Hyper-V ou SQL Server em SMB

Conclua a Planilha de configuração de volume

A Planilha fornece uma maneira fácil de Registrar os valores de que você precisa ao criar volumes para configurações do SQL Server e do Hyper-V em SMB.

Para cada volume, você deve especificar as seguintes informações:

- Nome da máquina virtual de storage (SVM)

O nome do SVM é o mesmo para todos os volumes.

- Nome do volume
- Nome agregado

  É possível criar volumes em agregados localizados em qualquer nó do cluster.

- Tamanho
- Caminho de junção

Você deve ter em mente o seguinte ao criar volumes usados para armazenar dados do servidor de aplicativos:

- Se o volume raiz não tiver um estilo de segurança NTFS, deve especificar o estilo de segurança como NTFS quando criar o volume.

  Por padrão, os volumes herdam o estilo de segurança do volume raiz da SVM.

- Os volumes devem ser configurados com a garantia de espaço de volume padrão.
- Opcionalmente, você pode configurar a configuração de gerenciamento de espaço de dimensionamento automático.
- Você deve definir a opção que determina a reserva de espaço de cópia Snapshot como `0`.
- A política Snapshot aplicada ao volume deve ser desativada.

  Se a política SVM Snapshot estiver desativada, você não precisará especificar uma política de Snapshot para os volumes. Os volumes herdam a política Snapshot da SVM. Se a política Snapshot do SVM não estiver desativada e estiver configurada para criar cópias Snapshot, você precisará especificar uma política de Snapshot no nível de volume e essa política deverá ser desativada. Os backups habilitados para o serviço de cópia sombra e os backups do SQL Server gerenciam a criação e exclusão de cópias Snapshot.

- Não é possível configurar espelhos de compartilhamento de carga para os volumes.

Os caminhos de junção nos quais você planeja criar compartilhamentos que os servidores de aplicativos usam devem ser escolhidos para que não haja volumes juntados abaixo do ponto de entrada de compartilhamento.

Por exemplo, se você quiser armazenar arquivos de máquina virtual em quatro volumes denominados "'vol1"", "'vol2", "'vol3" e "'vol4"", você pode criar o namespace mostrado no exemplo. Em seguida, é possível criar compartilhamentos para os servidores de aplicativos nos seguintes caminhos: `/data1/vol1`, `/data1/vol2`, `/data2/vol3` E `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Tipos de informação	Valores
Volume 1: Nome do volume, agregado, tamanho, caminho de junção	
Volume 2: Nome do volume, agregado, tamanho, caminho de junção	
Volume 3: Nome do volume, agregado, tamanho, caminho de junção	
Volume 4: Nome do volume, agregado, tamanho, caminho de junção	
Volume 5: Nome do volume, agregado, tamanho, caminho de junção	
Volume 6: Nome do volume, agregado, tamanho, caminho de junção	
Volumes adicionais: Nome do volume, agregado, tamanho, caminho de junção	

Conclua a Planilha de configuração do compartilhamento SMB

Use esta Planilha para Registrar os valores de que você precisa ao criar compartilhamentos SMB continuamente disponíveis para configurações do SQL Server e do Hyper-V sobre SMB.

Informações sobre as propriedades de compartilhamentos SMB e configurações

Para cada compartilhamento, você deve especificar as seguintes informações:

- Nome da máquina virtual de storage (SVM)

  O nome do SVM é o mesmo para todos os compartilhamentos

- Nome da partilha
- Caminho
- Compartilhar propriedades

  Você deve configurar as duas propriedades de compartilhamento a seguir:

  - `oplocks`
  - `continuously-available`

As seguintes propriedades de compartilhamento não devem ser definidas:

- `homedirectory attributecache`

- `branchcache`
- `access-based-enumeration`
  - Links simbólicos devem ser desativados (o valor para o `-symlink-properties` parâmetro deve ser nulo ["]).

Informações sobre caminhos de compartilhamento

Se você estiver usando o VSS remoto para fazer backup de arquivos Hyper-V, a escolha de caminhos de compartilhamento a serem usados ao fazer conexões SMB dos servidores Hyper-V para os locais de armazenamento onde os arquivos da máquina virtual são armazenados é importante. Embora os compartilhamentos possam ser criados em qualquer ponto do namespace, os caminhos para compartilhamentos que os servidores Hyper-V usam não devem conter volumes juntados. As operações de cópia sombra não podem ser executadas em caminhos de partilha que contenham pontos de junção.

O SQL Server não pode cruzar junções ao criar a estrutura do diretório do banco de dados. Você não deve criar caminhos de compartilhamento para o servidor SQL que contenham pontos de junção.

Por exemplo, dado o namespace mostrado, se você quiser armazenar arquivos de máquina virtual ou arquivos de banco de dados nos volumes "'vol1", "'vol2", "'vol3"" e "'vol4", você deve criar compartilhamentos para os servidores de aplicativos nos seguintes caminhos: `/data1/vol1`, , `/data1/vol2`, `/data2/vol3` E `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Embora seja possível criar compartilhamentos `/data1` nos caminhos e `/data2` para gerenciamento administrativo, não é necessário configurar os servidores de aplicativos para usar esses compartilhamentos para armazenar dados.

Folha de trabalho de planeamento

Tipos de informação	Valores
Volume 1: Nome e caminho do compartilhamento SMB	
Volume 2: Nome e caminho do compartilhamento SMB	
Volume 3: Nome e caminho do compartilhamento SMB	

Tipos de informação	Valores
Volume 4: Nome e caminho do compartilhamento SMB	
Volume 5: Nome e caminho do compartilhamento SMB	
Volume 6: Nome e caminho do compartilhamento SMB	
Volume 7: Nome e caminho do compartilhamento SMB	
Volumes adicionais: Nomes e caminhos de compartilhamento SMB	

Crie configurações de ONTAP para operações ininterruptas com Hyper-V e SQL Server em SMB

Crie configurações do ONTAP para operações ininterruptas com a visão geral do Hyper-V e do SQL Server sobre SMB

Há várias etapas de configuração do ONTAP que você deve executar para se preparar para instalações do Hyper-V e SQL Server que fornecem operações ininterruptas em SMB.

Antes de criar a configuração do ONTAP para operações ininterruptas com o Hyper-V e o SQL Server em SMB, as seguintes tarefas devem ser concluídas:

- Os serviços de tempo devem ser configurados no cluster.
- É necessário configurar uma rede para o SVM.
- É necessário criar o SVM.
- As interfaces de LIF de dados devem ser configuradas na SVM.
- O DNS deve ser configurado na SVM.
- Os serviços de nomes desejados devem ser configurados para o SVM.
- O servidor SMB deve ser criado.

Informações relacionadas

Planeje a configuração Hyper-V ou SQL Server em SMB

Requisitos e considerações de configuração

Verifique se a autenticação Kerberos e NTLMv2 são permitidas (Hyper-V sobre compartilhamentos SMB)

Operações ininterruptas para Hyper-V em SMB exigem que o servidor CIFS em um SVM de dados e o servidor Hyper-V permitam a autenticação Kerberos e NTLMv2. Você deve

verificar as configurações no servidor CIFS e nos servidores Hyper-V que controlam quais métodos de autenticação são permitidos.

Sobre esta tarefa

A autenticação Kerberos é necessária ao fazer uma conexão de compartilhamento continuamente disponível. Parte do processo VSS remoto usa autenticação NTLMv2.1X. Portanto, conexões usando ambos os métodos de autenticação devem ser suportadas para configurações Hyper-V em SMB.

As seguintes configurações devem ser configuradas para permitir a autenticação Kerberos e NTLMv2:

- As políticas de exportação para SMB devem ser desativadas na máquina virtual de storage (SVM).

A autenticação Kerberos e NTLMv2 estão sempre ativadas em SVMs, mas as políticas de exportação podem ser usadas para restringir o acesso com base no método de autenticação.

As políticas de exportação para SMB são opcionais e estão desativadas por padrão. Se as políticas de exportação estiverem desativadas, a autenticação Kerberos e NTLMv2 serão permitidas em um servidor CIFS por padrão.

- O domínio ao qual o servidor CIFS e os servidores Hyper-V pertencem deve permitir a autenticação Kerberos e NTLMv2.

A autenticação Kerberos é ativada por padrão em domínios do ative Directory. No entanto, a autenticação NTLMv2.1X pode ser desativada, utilizando as definições de Política de Segurança ou políticas de Grupo.

Passos

1. Execute o seguinte procedimento para verificar se as políticas de exportação estão desativadas no SVM:
   a. Defina o nível de privilégio como avançado:

      ```
      set -privilege advanced
      ```

   b. Verifique se a `-is-exportpolicy-enabled` opção de servidor CIFS está definida como `false`:

      ```
      vserver cifs options show -vserver vserver_name -fields vserver,is-
      exportpolicy-enabled
      ```

   c. Voltar ao nível de privilégio de administrador:

      ```
      set -privilege admin
      ```

2. Se as políticas de exportação para SMB não estiverem desativadas, desative-as:

   ```
   vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled
   false
   ```

3. Verifique se a autenticação NTLMv2 e Kerberos são permitidas no domínio.

   Para obter informações sobre como determinar quais métodos de autenticação são permitidos no domínio, consulte a Biblioteca Microsoft TechNet.

4. Se o domínio não permitir a autenticação NTMLv2.1x, ative a autenticação NTLMv2.1x utilizando um dos métodos descritos na documentação da Microsoft.

Exemplo

Os comandos a seguir verificam se as políticas de exportação para SMB estão desativadas no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ----------------------
vs1      false

cluster1::*> set -privilege admin
```

Verifique se as contas de domínio são mapeadas para o usuário UNIX padrão

Hyper-V e SQL Server usam contas de domínio para criar conexões SMB para compartilhamentos continuamente disponíveis. Para criar a conexão com êxito, a conta do computador deve mapear com êxito para um usuário UNIX. A maneira mais conveniente de fazer isso é mapear a conta do computador para o usuário UNIX padrão.

Sobre esta tarefa

Hyper-V e SQL Server usam as contas de computador de domínio para criar conexões SMB. Além disso, o SQL Server usa uma conta de usuário de domínio como a conta de serviço que também faz conexões SMB.

Quando você cria uma máquina virtual de armazenamento (SVM), o ONTAP cria automaticamente o usuário padrão chamado "'pcuser'" (com um UID do `65534`) e o grupo chamado "'pcuser'" (com um GID do `65534`) e adiciona o usuário padrão ao grupo "'pcuser'". Se você estiver configurando uma solução Hyper-V sobre SMB em um SVM que existia antes de atualizar o cluster para o Data ONTAP 8.2, o usuário e o grupo padrão podem não existir. Se não o fizerem, você deverá criá-los antes de configurar o usuário UNIX padrão do servidor CIFS.

Passos

1. Determine se há um usuário UNIX padrão:

   vserver cifs options show -vserver *vserver_name*

2. Se a opção de usuário padrão não estiver definida, determine se há um usuário UNIX que pode ser designado como o usuário UNIX padrão:

   vserver services unix-user show -vserver *vserver_name*

3. Se a opção de usuário padrão não estiver definida e não houver um usuário UNIX que possa ser designado como usuário UNIX padrão, crie o usuário UNIX padrão e o grupo padrão e adicione o usuário padrão ao grupo.

   Geralmente, o usuário padrão recebe o nome de usuário ""pcuser"" e deve ser atribuído o UID de `65534`.

O grupo padrão geralmente recebe o nome do grupo ""pcuser"". O GID atribuído ao grupo deve ser `65534`.

a. Criar o grupo padrão
vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534

b. Crie o usuário padrão e adicione o usuário padrão ao grupo padrão
vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534

c. Verifique se o usuário padrão e o grupo padrão estão configurados corretamente
vserver services unix-user show -vserver *vserver_name*
vserver services unix-group show -vserver *vserver_name* -members

4. Se o usuário padrão do servidor CIFS não estiver configurado, execute o seguinte procedimento:

a. Configurar o utilizador predefinido:

vserver cifs options modify -vserver *vserver_name* `-default-unix-user pcuser*`

b. Verifique se o usuário UNIX padrão está configurado corretamente:

vserver cifs options show -vserver *vserver_name*

5. Para verificar se a conta do computador do servidor de aplicativos mapeia corretamente para o usuário padrão, mapeie uma unidade para um compartilhamento residente no SVM e confirme o mapeamento do usuário do Windows para o UNIX usando o `vserver cifs session show` comando.

Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Exemplo

Os comandos a seguir determinam que o usuário padrão do servidor CIFS não está definido, mas determina que o usuário "'pcuser'" e o grupo "'pcuser'" existem. O usuário "'pcuser'" é atribuído como o usuário padrão do servidor CIFS na SVM VS1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
```

```
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Verifique se o estilo de segurança do volume raiz SVM está definido como NTFS

Para garantir que as operações ininterruptas para Hyper-V e SQL Server sobre SMB sejam bem-sucedidas, os volumes devem ser criados com o estilo de segurança NTFS. Como o estilo de segurança do volume raiz é aplicado por padrão aos volumes criados na máquina virtual de armazenamento (SVM), o estilo de segurança do volume raiz deve ser definido como NTFS.

Sobre esta tarefa

- Você pode especificar o estilo de segurança do volume raiz no momento em que você criar o SVM.
- Se o SVM não for criado com o volume raiz definido como estilo de segurança NTFS, você poderá alterar o estilo de segurança mais tarde usando o `volume modify` comando.

Passos

1. Determine o estilo de segurança atual do volume raiz da SVM:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. Se o volume raiz não for um volume de estilo de segurança NTFS, altere o estilo de segurança para NTFS:

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Verifique se o volume raiz SVM está definido como estilo de segurança NTFS:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Exemplo

Os comandos a seguir verificam se o estilo de segurança do volume raiz é NTFS no SVM VS1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Verifique se as opções de servidor CIFS necessárias estão configuradas

Você deve verificar se as opções de servidor CIFS necessárias estão habilitadas e configuradas de acordo com os requisitos para operações ininterruptas para Hyper-V e SQL Server sobre SMB.

Sobre esta tarefa

- O SMB 2.x e o SMB 3,0 devem estar ativados.
- A descarga de cópia ODX deve ser habilitada para usar a descarga de cópia que melhora o desempenho.
- Os serviços VSS Shadow Copy devem estar ativados se a solução Hyper-V over SMB utilizar serviços de cópia de segurança ativados por VSS remoto (apenas Hyper-V).

Passos

1. Verifique se as opções de servidor CIFS necessárias estão ativadas na máquina virtual de armazenamento (SVM):
   a. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

b. Introduza o seguinte comando:

```
vserver cifs options show -vserver vserver_name
```

As seguintes opções devem ser definidas como `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Apenas Hyper-V)

2. Se alguma das opções não estiver definida como `true`, execute o seguinte procedimento:
   a. Defina-os como `true` utilizando o `vserver cifs options modify` comando.
   b. Verifique se as opções estão definidas `true` usando o `vserver cifs options show` comando.
3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

Os comandos a seguir verificam se as opções necessárias para a configuração Hyper-V sobre SMB estão habilitadas no SVM VS1. No exemplo, a descarga de cópia ODX deve estar habilitada para atender aos requisitos de opção.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configure o SMB Multichannel para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas para configurações Hyper-V e SQL Server em SMB.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

  O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

  O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilégio avançado):

- `-max-connections-per-session`

  O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

  Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

  O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Ative SMB Multichannel no servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

```
vserver cifs session show
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
       Workstation IP Address: 10.1.1.1
      Authentication Mechanism: NTLMv1
         User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Criar volumes de dados NTFS

Você deve criar volumes de dados NTFS na máquina virtual de armazenamento (SVM) antes de poder configurar compartilhamentos continuamente disponíveis para uso com

Hyper-V ou SQL Server em servidores de aplicativos SMB. Use a Planilha de configuração de volume para criar seus volumes de dados.

Sobre esta tarefa

Há parâmetros opcionais que você pode usar para personalizar um volume de dados. Para obter mais informações sobre a personalização de volumes, consulte "Gerenciamento de storage lógico".

À medida que você cria seus volumes de dados, você não deve criar pontos de junção dentro de um volume que contenha o seguinte:

- Arquivos Hyper-V para os quais o ONTAP faz cópias de sombra
- Arquivos de banco de dados do SQL Server que são copiados usando o SQL Server

> Se você inadvertidamente criar um volume que usa estilo de segurança misto ou UNIX, não poderá alterar o volume para um volume de estilo de segurança NTFS e usá-lo diretamente para criar compartilhamentos continuamente disponíveis para operações ininterruptas. Operações ininterruptas para Hyper-V e SQL Server em SMB não funcionam corretamente, a menos que os volumes usados na configuração sejam criados como volumes de estilo de segurança NTFS. Você deve excluir o volume e recriar o volume com estilo de segurança NTFS, ou pode mapear o volume em um host Windows e aplicar uma ACL na parte superior do volume e propagar a ACL para todos os arquivos e pastas no volume.

Passos

1. Crie o volume de dados inserindo o comando apropriado:

Se você quiser criar um volume em um SVM onde o estilo de segurança do volume raiz é…	Digite o comando…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Não NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. Verifique se a configuração do volume está correta:

   `volume show -vserver vserver_name -volume volume_name`

Crie compartilhamentos SMB continuamente disponíveis

Depois de criar seus volumes de dados, você pode criar os compartilhamentos continuamente disponíveis que os servidores de aplicativos usam para acessar a máquina virtual Hyper-V e os arquivos de configuração e os arquivos de banco de dados do SQL Server. Você deve usar a Planilha de configuração de compartilhamento ao criar

compartilhamentos SMB.

Passos

1. Apresenta informações sobre os volumes de dados existentes e os respetivos caminhos de junção:

   volume show -vserver *vserver_name* -junction

2. Crie um compartilhamento SMB continuamente disponível:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - Opcionalmente, você pode adicionar um comentário à configuração de compartilhamento.
   - Por padrão, a propriedade de compartilhamento de arquivos off-line é configurada no compartilhamento e está definida como `manual`.
   - O ONTAP cria o compartilhamento com a permissão de compartilhamento padrão do Windows de `Everyone` / `Full Control`.

3. Repita a etapa anterior para todos os compartilhamentos na Planilha de configuração de compartilhamento.
4. Verifique se sua configuração está correta usando o `vserver cifs share show` comando.
5. Configure permissões de arquivo NTFS nos compartilhamentos continuamente disponíveis mapeando uma unidade para cada compartilhamento e configurando permissões de arquivo usando a janela **Propriedades do Windows**.

Exemplo

Os comandos a seguir criam um compartilhamento continuamente disponível chamado "ata2" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Os links simbólicos são desativados definindo o `-symlink` parâmetro para `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Adicionar o privilégio SeSecurityPrivilege à conta de usuário (para SQL Server de compartilhamentos SMB)

A conta de usuário do domínio usada para instalar o servidor SQL deve ser atribuída ao privilégio ""SeSecurityPrivilege"" para executar determinadas ações no servidor CIFS que exigem Privileges não atribuído por padrão aos usuários do domínio.

O que você vai precisar

A conta de domínio usada para instalar o SQL Server já deve existir.

Sobre esta tarefa

Ao adicionar o privilégio à conta do instalador do SQL Server, o ONTAP pode validar a conta entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Adicione o privilégio "SeSecurityPrivilege":

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   O valor para o `-user-or-group-name` parâmetro é o nome da conta de usuário do domínio usada para instalar o SQL Server.

2. Verifique se o privilégio é aplicado à conta:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Exemplo

O comando a seguir adiciona o privilégio "'SeSecurityPrivilege" à conta do instalador do SQL Server no domínio DE EXEMPLO para máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

Configurar a profundidade do diretório de cópia de sombra VSS (para compartilhamentos Hyper-V sobre SMB)

Opcionalmente, você pode configurar a profundidade máxima de diretórios em compartilhamentos SMB nos quais criar cópias sombra. Este parâmetro é útil se você quiser controlar manualmente o nível máximo de subdiretórios nos quais o ONTAP deve criar cópias de sombra.

O que você vai precisar

O recurso de cópia de sombra VSS deve estar ativado.

Sobre esta tarefa

O padrão é criar cópias de sombra para um máximo de cinco subdiretórios. Se o valor estiver definido como `0`, o ONTAP criará cópias de sombra para todos os subdiretórios.

> Embora você possa especificar que a profundidade do diretório do conjunto de cópias de sombra inclua mais de cinco subdiretórios ou todos os subdiretórios, há um requisito da Microsoft de que a criação do conjunto de cópias de sombra deve ser concluída em 60 segundos. A criação do conjunto de cópias de sombra falhará se não puder ser concluída dentro deste período de tempo. A profundidade do diretório de cópia sombra escolhida não deve fazer com que o tempo de criação exceda o limite de tempo.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Defina a profundidade do diretório de cópia de sombra VSS para o nível desejado:

   `vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer`

   `vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6`

3. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Gerenciar configurações do Hyper-V e do SQL Server em SMB

Configurar compartilhamentos existentes para disponibilidade contínua

Você pode modificar compartilhamentos existentes para se tornarem compartilhamentos continuamente disponíveis que os servidores de aplicativos Hyper-V e SQL Server usam para acessar arquivos de configuração e máquina virtual Hyper-V sem interrupções e arquivos de banco de dados do SQL Server.

Sobre esta tarefa

Você não pode usar um compartilhamento existente como um compartilhamento continuamente disponível para operações ininterruptas com servidores de aplicações em SMB se o compartilhamento tiver as seguintes características:

- Se a `homedirectory` propriedade share estiver definida nesse compartilhamento
- Se o compartilhamento contiver links simbólicos ou widelinks habilitados
- Se o compartilhamento contiver volumes juntados abaixo da raiz do compartilhamento

Você deve verificar se os dois parâmetros de compartilhamento a seguir estão definidos corretamente:

- O `-offline-files` parâmetro é definido como `manual` (o padrão) ou `none`.
- Os links simbólicos devem ser desativados.

As seguintes propriedades de compartilhamento devem ser configuradas:

- `continuously-available`
- `oplocks`

As seguintes propriedades de compartilhamento não devem ser definidas. Se eles estiverem presentes na lista de propriedades de compartilhamento atuais, eles precisam ser removidos do compartilhamento continuamente disponível:

- `attributecache`
- `branchcache`

Passos

1. Exiba as configurações atuais de parâmetros de compartilhamento e a lista atual de propriedades de compartilhamento configuradas:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Se necessário, modifique os parâmetros de compartilhamento para desativar links simbólicos e defina arquivos off-line para manual usando o `vserver cifs share modify` comando.
   - Pode desativar os links simbólicos definindo o valor do `-symlink` parâmetro para `""`.
   - Pode definir o `-offline-files` parâmetro para a definição correta especificando `manual`.
3. Adicione a `continuously-available` propriedade da ação e, se necessário, a `oplocks` propriedade da ação:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Se a `oplocks` propriedade share ainda não estiver definida, você deve adicioná-la juntamente com a `continuously-available` propriedade share.

4. Remova quaisquer propriedades de compartilhamento que não sejam suportadas em compartilhamentos disponíveis continuamente:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   Você pode remover uma ou mais propriedades de compartilhamento especificando as propriedades de compartilhamento com uma lista delimitada por vírgulas.

5. Verifique se `-symlink` os parâmetros e `-offline-files` estão definidos corretamente:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Verifique se a lista de propriedades de compartilhamento configuradas está correta:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Exemplos

O exemplo a seguir mostra como configurar um compartilhamento existente chamado "share1" na máquina virtual de armazenamento (SVM) "VS1" para NDOs com um servidor de aplicativos sobre SMB:

- Os links simbólicos são desativados no compartilhamento definindo o `-symlink` parâmetro como `""`.
- O `-offline-file` parâmetro é modificado e definido para `manual`.
- A `continuously-available` propriedade share é adicionada à ação.
- A `oplocks` propriedade da ação já está na lista de propriedades da ação; portanto, ela não precisa ser adicionada.
- A `attributecache` propriedade share é removida da ação.
- A `browsable` propriedade de compartilhamento é opcional para um compartilhamento continuamente disponível usado para NDOs com servidores de aplicativos em SMB e é mantido como uma das propriedades de compartilhamento.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Ative ou desative cópias de sombra VSS para backups Hyper-V em SMB

Se você usar um aplicativo de backup com reconhecimento VSS para fazer backup de arquivos de máquina virtual Hyper-V armazenados em compartilhamentos SMB, a cópia de sombra VSS deve estar habilitada. Você pode desativar a cópia de sombra do VSS se não usar aplicativos de backup com reconhecimento VSS. O padrão é ativar a cópia de sombra VSS.

Sobre esta tarefa

Você pode ativar ou desativar cópias de sombra VSS a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser que cópias de sombra VSS sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

Os comandos a seguir habilitam cópias de sombra do VSS no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Use estatísticas para monitorar a atividade do Hyper-V e do SQL Server em SMB

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser determinar…	Digite…
Quais objetos estão disponíveis	`statistics catalog object show`
Objetos específicos que estão disponíveis	`statistics catalog object show object` *`object_name`*
Quais contadores estão disponíveis	`statistics catalog counter show object` *`object_name`*

   Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível de privilégio avançado:

> Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Exibir estatísticas SMB no ONTAP

Você pode exibir várias estatísticas SMB para monitorar o desempenho e diagnosticar

problemas.

Passos

1. Use os `statistics start` comandos e opcionais `statistics stop` para coletar uma amostra de dados.
2. Execute uma das seguintes ações:

Se você quiser exibir estatísticas para…	Digite o seguinte comando…
Todas as versões do SMB	**`statistics show -object cifs`**
SMB 1,0	**`statistics show -object smb1`**
SMB 2.x e SMB 3,0	**`statistics show -object smb2`**
Subsistema SMB do nó	**`statistics show -object nblade_cifs`**

Saiba mais sobre os comandos link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-show.html[`statistics show`(em inglês), link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-start.html[`statistics start`(em inglês) e link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-stop.html[`statistics stop`(em inglês) na referência de comando ONTAP.

Verifique se a configuração é capaz de operações ininterruptas

Use o monitoramento de integridade para determinar se o status de operação sem interrupções está íntegro

O monitoramento de integridade fornece informações sobre o status de integridade do sistema em todo o cluster. O monitor de integridade monitora as configurações Hyper-V e SQL Server em SMB para garantir operações ininterruptas (NDOs) para os servidores de aplicações. Se o estado estiver degradado, pode visualizar detalhes sobre o problema, incluindo a causa provável e as ações de recuperação recomendadas.

Existem vários monitores de saúde. O ONTAP monitora a integridade e a integridade geral do sistema para monitores de integridade individuais. O monitor de integridade da conetividade do nó contém o subsistema CIFS-NDO. O monitor tem um conjunto de políticas de integridade que acionam alertas se certas condições físicas podem causar interrupções e, se houver uma condição disruptiva, gera alertas e fornece informações sobre ações corretivas. Para configurações NDO sobre SMB, alertas são gerados para as duas condições a seguir:

ID de alerta	Gravidade	Condição
HaNotReadyCifsNdo_Alert	Maior	Um ou mais arquivos hospedados por um volume em um agregado no nó foram abertos por meio de um compartilhamento SMB continuamente disponível com a promessa de persistência em caso de falha. No entanto, o relacionamento de HA com o parceiro não está configurado ou não está íntegro.
NoStandbyLifCifsNdo_Alert	Menor	A máquina virtual de storage (SVM) está fornecendo dados ativamente sobre SMB por meio de um nó e há arquivos SMB abertos persistentemente por compartilhamentos disponíveis continuamente. No entanto, seu nó de parceiro não expõe LIFs de dados ativos para o SVM.

Exibir o status de operação sem interrupções usando o monitoramento de integridade do sistema

Você pode usar os `system health` comandos para exibir informações sobre a integridade geral do sistema do cluster e a integridade do subsistema CIFS-NDO, responder a alertas, configurar alertas futuros e exibir informações sobre como o monitoramento de integridade está configurado.

Passos

1. Monitore o status de integridade executando a ação apropriada:

Se você quiser exibir…	Digite o comando…
O estado de saúde do sistema, que reflete o estado geral dos monitores de saúde individuais	**system health status show**
Informações sobre o estado de funcionamento do subsistema CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Exiba informações sobre como o monitoramento de alerta CIFS-NDO é configurado executando as ações apropriadas:

Se você quiser exibir informações sobre…	Digite o comando…
A configuração e o status do monitor de integridade do subsistema CIFS-NDO, como nós monitorados, estado de inicialização e status	**system health config show -subsystem CIFS-NDO**

Se você quiser exibir informações sobre…	Digite o comando…
O CIFS-NDO alerta que um monitor de integridade pode gerar	**system health alert definition show -subsystem CIFS-NDO**
Políticas do monitor de integridade CIFS-NDO, que determinam quando os alertas são gerados	**system health policy definition show -monitor node-connect**

Use o `-instance` parâmetro para exibir informações detalhadas.

Exemplos

A saída a seguir mostra informações sobre o status geral de integridade do cluster e do subsistema CIFS-NDO:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

A saída a seguir mostra informações detalhadas sobre a configuração e o status do monitor de integridade do subsistema CIFS-NDO:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Verifique a configuração de compartilhamento SMB continuamente disponível

Para dar suporte a operações ininterruptas, os compartilhamentos SMB do Hyper-V e do SQL Server devem ser configurados como compartilhamentos disponíveis continuamente. Além disso, existem certas outras configurações de compartilhamento que você deve verificar. Você deve verificar se os compartilhamentos estão configurados corretamente para fornecer operações ininterruptas contínuas para os servidores de aplicações, se houver eventos disruptivos planejados ou não planejados.

Sobre esta tarefa

Você deve verificar se os dois parâmetros de compartilhamento a seguir estão definidos corretamente:

- O `-offline-files` parâmetro é definido como `manual` (o padrão) ou `none`.
- Os links simbólicos devem ser desativados.

Para operações ininterruptas adequadas, as seguintes propriedades de compartilhamento devem ser definidas:

- `continuously-available`
- `oplocks`

As seguintes propriedades de compartilhamento não devem ser definidas:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Passos

1. Verifique se os arquivos off-line estão definidos como `manual` ou `disabled` e se os links simbólicos estão desativados:

   vserver cifs shares show -vserver *vserver_name*

2. Verifique se os compartilhamentos SMB estão configurados para disponibilidade contínua:

   vserver cifs shares properties show -vserver *vserver_name*

Exemplos

O exemplo a seguir exibe a configuração de compartilhamento para um compartilhamento chamado "hare1" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Os arquivos offline são definidos como `manual` e os links simbólicos são desativados (designados por um hífen na `Symlink Properties` saída do campo):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

O exemplo a seguir exibe as propriedades de compartilhamento de um compartilhamento chamado "hare1" no SVM VS1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Verifique o status do LIF

Mesmo que você configure máquinas virtuais de armazenamento (SVMs) com configurações Hyper-V e SQL Server sobre SMB para ter LIFs em cada nó em um cluster, durante operações diárias, alguns LIFs podem se mover para portas em outro nó. Você deve verificar o status do LIF e tomar todas as ações corretivas necessárias.

Sobre esta tarefa

Para oferecer suporte contínuo a operações ininterruptas e sem interrupções, cada nó em um cluster precisa ter pelo menos um LIF para a SVM e todos os LIFs precisam estar associados a uma porta inicial. Se algumas LIFs configuradas não estiverem associadas atualmente à porta inicial, você deverá corrigir quaisquer problemas de porta e reverter os LIFs para a porta inicial.

Passos

1. Exibir informações sobre LIFs configuradas para o SVM:

   `network interface show -vserver` *`vserver_name`*

   Neste exemplo, "'lif1'" não está localizado na porta inicial.

```
network interface show -vserver vs1
```

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

2. Se alguns dos LIFs não estiverem em suas portas residenciais, execute as seguintes etapas:

   a. Para cada LIF, determine qual é a porta inicial do LIF:

   network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

   ```
   vserver lif  home-node  home-port
   ------- ---- ---------- ---------
   vs1     lif1 node1      e0d
   ```

   b. Para cada LIF, determine se a porta inicial do LIF está ativa:

   network port show -node *node_name* -port *port* -fields port,link

   ```
   network port show -node node1 -port e0d -fields port,link
   ```

   ```
   node       port link
   ---------- ---- ----
   node1      e0d  up
   ```

   +
   Neste exemplo, "'lif1" deve ser migrado de volta para sua porta de origem, `node1:e0d`.

3. Se qualquer uma das interfaces de rede de porta inicial às quais os LIFs devem estar associados não estiver no `up` estado, resolva o problema para que essas interfaces estejam ativas.
4. Se necessário, reverta os LIFs para suas portas residenciais:

   network interface revert -vserver *vserver_name* -lif *lif_name*

```
network interface revert -vserver vs1 -lif lif1
```

5. Verifique se cada nó no cluster tem um LIF ativo para o SVM:

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determine se as sessões SMB estão continuamente disponíveis

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

  Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
Para todas as sessões no SVM de forma resumida	**vserver cifs session show -vserver *vserver_name***
Em um ID de conexão especificado	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
A partir de um endereço IP de estação de trabalho especificado	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Em um endereço IP de LIF especificado	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Em um nó especificado	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	De um usuário do Windows especificado
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* O formato para `user_name` é `[domain]\user`.	Com um mecanismo de autenticação especificado

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism O valor para `-auth -mechanism` pode ser um dos seguintes: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Com uma versão de protocolo especificada

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version O valor para `-protocol-version` pode ser um dos seguintes: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Com um nível especificado de proteção continuamente disponível

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
`vserver cifs session show -vserver vserver_name -continuously -available continuously_available_protection_level` O valor para `-continuously -available` pode ser um dos seguintes: • `No` • `Yes` • `Partial` Se o status continuamente disponível for `Partial`, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode	Com um status de sessão de assinatura SMB especificado

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço IP 10,1.1,1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281 1       10.1.1.1         DOMAIN\joe          2          23s
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                      Node: node1
                   Vserver: vs1
                Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
             Windows User: DOMAIN\SERVER1$
                UNIX User: pcuser
              Open Shares: 1
               Open Files: 1
               Open Other: 0
            Connected Time: 10m 43s
                 Idle Time: 1m 19s
          Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conetado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conetar com a proteção continuamente disponível.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você também pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show` comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais

informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
No SVM no formulário de resumo	**vserver cifs session file show -vserver *vserver_name***
Em um nó especificado	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Em um ID de arquivo especificado
vserver cifs session file show -vserver *vserver_name* -file-id integer	Em uma ID de conexão SMB especificada
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Em um SMB Session ID especificado
vserver cifs session file show -vserver *vserver_name* -session-id integer	No agregado de hospedagem especificado
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	No volume especificado
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	No compartilhamento SMB especificado
vserver cifs session file show -vserver *vserver_name* -share *share_name*	No caminho SMB especificado

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
vserver cifs session file show -vserver *vserver_name* -path *path*	Com o nível especificado de proteção continuamente disponível
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* O valor para `-continuously-available` pode ser um dos seguintes: • `No` • `Yes` Se o status continuamente disponível for `No`, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade.	Com o estado de reconexão especificado

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Gerenciamento de STORAGE SAN

Conceitos de SAN

Provisionamento DE SAN com iSCSI

Em ambientes SAN, os sistemas de armazenamento são alvos que têm dispositivos de armazenamento de destino. Para iSCSI e FC, os dispositivos de destino de armazenamento são referidos como LUNs (unidades lógicas). Para Non-Volatile Memory Express (NVMe) em Fibre Channel, os dispositivos de destino de storage são chamados de namespaces.

Você configura o storage criando LUNs para iSCSI e FC ou criando namespaces para NVMe. Os LUNs ou namespaces são então acessados por hosts que usam redes de protocolo iSCSI (Internet Small Computer Systems Interface) ou Fibre Channel (FC).

Para se conetar a redes iSCSI, os hosts podem usar placas de rede Ethernet (NICs) padrão, TOE (TCP offload Engine) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host iSCSI dedicados (HBAs).

Para se conetar a redes FC, os hosts exigem HBAs FC ou CNAs.

Os protocolos FC compatíveis incluem:

- FC
- FCoE
- NVMe

Ligações e nomes de rede de nó de destino iSCSI

Os nós de destino iSCSI podem se conetar à rede de várias maneiras:

- Interfaces over Ethernet usando software integrado ao ONTAP.
- Em várias interfaces de sistema, com uma interface usada para iSCSI que também pode transmitir tráfego para outros protocolos, como SMB e NFS.
- Usando um adaptador de destino unificado (UTA) ou um adaptador de rede convergente (CNA).

Cada nó iSCSI deve ter um nome de nó.

Os dois formatos, ou designadores de tipo, para nomes de nós iSCSI são *iqn* e *eui*. O destino SVM iSCSI sempre usa o designador do tipo iqn. O iniciador pode usar o designador iqn-type ou eui-type.

Nome do nó do sistema de storage

Cada SVM que executa iSCSI tem um nome de nó padrão com base em um nome de domínio reverso e um número de codificação exclusivo.

O nome do nó é exibido no seguinte formato:

iqn.1992-08.com.NetApp:sn.*unique-encoding-number*

O exemplo a seguir mostra o nome do nó padrão para um sistema de armazenamento com um número de codificação exclusivo:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Porta TCP para iSCSI

O protocolo iSCSI está configurado no ONTAP para utilizar a porta TCP número 3260.

O ONTAP não suporta a alteração do número da porta para iSCSI. A porta número 3260 está registada como parte da especificação iSCSI e não pode ser utilizada por qualquer outra aplicação ou serviço.

Informações relacionadas

"Documentação do NetApp: Configuração do host SAN ONTAP"

Gerenciamento de serviços iSCSI

Gerenciamento de serviços iSCSI

Você pode gerenciar a disponibilidade do serviço iSCSI nas interfaces lógicas iSCSI da máquina virtual de storage (SVM) usando os `vserver iscsi interface enable` comandos ou `vserver iscsi interface disable`.

Por predefinição, o serviço iSCSI está ativado em todas as interfaces lógicas iSCSI.

Como o iSCSI é implementado no host

O iSCSI pode ser implementado no host usando hardware ou software.

Você pode implementar iSCSI de uma das seguintes maneiras:

- Usando o software Initiator que usa as interfaces Ethernet padrão do host.
- Através de um adaptador de barramento de host iSCSI (HBA): Um HBA iSCSI aparece para o sistema operacional do host como um adaptador de disco SCSI com discos locais.
- Usando um adaptador TOE (TCP Offload Engine) que descarrega o processamento TCP/IP.

  O processamento do protocolo iSCSI ainda é realizado pelo software anfitrião.

Como a autenticação iSCSI funciona

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar uma sessão iSCSI. O sistema de armazenamento permite ou nega a solicitação de login ou determina que não é necessário fazer login.

Os métodos de autenticação iSCSI são:

- Challenge Handshake Authentication Protocol (CHAP) - o iniciador faz login usando um nome de usuário e senha CHAP.

Você pode especificar uma senha CHAP ou gerar uma senha secreta hexadecimal. Existem dois tipos de nomes de usuário CHAP e senhas:

  - Entrada - o sistema de armazenamento autentica o iniciador.

    As configurações de entrada são necessárias se você estiver usando a autenticação CHAP.

  - Outbound — esta é uma configuração opcional para permitir que o iniciador autentique o sistema de armazenamento.

    Só pode utilizar as definições de saída se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento.

- Negar - o iniciador tem acesso negado ao sistema de armazenamento.
- Nenhum - o sistema de storage não requer autenticação para o iniciador.

Pode definir a lista de iniciadores e os respetivos métodos de autenticação. Você também pode definir um método de autenticação padrão que se aplica a iniciadores que não estão nesta lista.

Informações relacionadas

"Opções de multipathing do Windows com Data ONTAP: Fibre Channel e iSCSI"

Gerenciamento de segurança do iniciador iSCSI

O ONTAP fornece uma série de recursos para gerenciar a segurança para iniciadores iSCSI. Pode definir uma lista de iniciadores iSCSI e o método de autenticação para cada um, apresentar os iniciadores e os respetivos métodos de autenticação associados na lista de autenticação, adicionar e remover iniciadores da lista de autenticação e definir o método de autenticação do iniciador iSCSI predefinido para iniciadores que não estão na lista.

Isolamento do ponto de extremidade iSCSI

A partir do ONTAP 9.1, os comandos de segurança iSCSI existentes foram melhorados para aceitar um intervalo de endereços IP ou vários endereços IP.

Todos os iniciadores iSCSI devem fornecer endereços IP de origem ao estabelecer uma sessão ou conexão com um destino. Essa nova funcionalidade impede que um iniciador faça login no cluster se o endereço IP de origem não for suportado ou desconhecido, fornecendo um esquema de identificação exclusivo. Qualquer iniciador originado de um endereço IP não suportado ou desconhecido terá seu login rejeitado na camada de sessão iSCSI, impedindo que o iniciador acesse qualquer LUN ou volume dentro do cluster.

Implemente essa nova funcionalidade com dois novos comandos para ajudar a gerenciar entradas pré-existentes.

Adicionar intervalo de endereços do iniciador

Melhore o gerenciamento de segurança do iniciador iSCSI adicionando um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Remova o intervalo de endereços do iniciador

Remova um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security remove-initiator-address-range` comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

O que é a autenticação CHAP

O CHAP (Challenge Handshake Authentication Protocol) permite a comunicação autenticada entre iniciadores e destinos iSCSI. Quando você usa autenticação CHAP, você define nomes de usuário CHAP e senhas tanto no iniciador quanto no sistema de armazenamento.

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar a sessão. A solicitação de login inclui o nome de usuário CHAP do iniciador e o algoritmo CHAP. O sistema de armazenamento responde com um desafio CHAP. O iniciador fornece uma resposta CHAP. O sistema de armazenamento verifica a resposta e autentica o iniciador. A senha CHAP é usada para calcular a resposta.

Diretrizes para o uso da autenticação CHAP

Você deve seguir certas diretrizes ao usar a autenticação CHAP.

- Se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de saída no iniciador. Se também definir um nome de utilizador e uma palavra-passe de saída no sistema de armazenamento para ativar a autenticação bidirecional, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de entrada no iniciador.
- Você não pode usar o mesmo nome de usuário e senha para configurações de entrada e saída no sistema de armazenamento.
- Os nomes de usuário CHAP podem ser de 1 a 128 bytes.

  Um nome de usuário nulo não é permitido.

- As senhas CHAP (segredos) podem ter 1 a 512 bytes.

  As senhas podem ser valores hexadecimais ou strings. Para valores hexadecimais, você deve inserir o valor com um prefixo "'0x'" ou "'0x'". Não é permitida uma palavra-passe nula.

> O ONTAP permite o uso de carateres especiais, letras não inglesas, números e espaços para senhas CHAP (segredos). No entanto, isso está sujeito a restrições de host. Se algum destes não for permitido pelo seu anfitrião específico, não poderão ser utilizados.
>
> Por exemplo, o iniciador de software iSCSI da Microsoft requer que as senhas CHAP do iniciador e do destino tenham pelo menos 12 bytes se a criptografia IPsec não estiver sendo usada. O comprimento máximo da senha é de 16 bytes, independentemente de o IPsec ser usado.
>
> Para restrições adicionais, você deve ver a documentação do iniciador.

Como usar listas de acesso à interface iSCSI para limitar as interfaces do iniciador pode aumentar o desempenho e a segurança

As listas de acesso à interface ISCSI podem ser usadas para limitar o número de LIFs em uma SVM que um iniciador pode acessar, aumentando assim a performance e a segurança.

Quando um iniciador inicia uma sessão de descoberta usando um comando iSCSI `SendTargets`, ele recebe os endereços IP associados ao LIF (interface de rede) que está na lista de acesso. Por padrão, todos os iniciadores têm acesso a todas as LIFs iSCSI na SVM. Você pode usar a lista de acesso para restringir o número de LIFs em uma SVM a que um iniciador tem acesso.

Serviço de nomes de armazenamento de Internet (iSNS)

O iSNS (Internet Storage Name Service) é um protocolo que permite a deteção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento TCP/IP. Um servidor iSNS mantém informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI IQN e grupos de portais.

Você pode obter um servidor iSNS de um fornecedor terceirizado. Se você tiver um servidor iSNS na rede configurado e habilitado para uso pelo iniciador e destino, poderá usar o LIF de gerenciamento de uma máquina virtual de armazenamento (SVM) para Registrar todos os LIFs iSCSI para esse SVM no servidor iSNS. Depois que o Registro estiver concluído, o iniciador iSCSI pode consultar o servidor iSNS para descobrir todos os LIFs para esse SVM específico.

Se você decidir usar um serviço iSNS, deve garantir que suas máquinas virtuais de armazenamento (SVMs) estejam registradas corretamente em um servidor iSNS (Internet Storage Name Service).

Se você não tiver um servidor iSNS na rede, você deverá configurar manualmente cada destino para ser visível para o host.

O que um servidor iSNS faz

Um servidor iSNS usa o protocolo iSNS (Internet Storage Name Service) para manter informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI (IQNs) e grupos de portais.

O protocolo iSNS permite a deteção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento IP. Um iniciador iSCSI pode consultar o servidor iSNS para descobrir dispositivos de destino iSCSI.

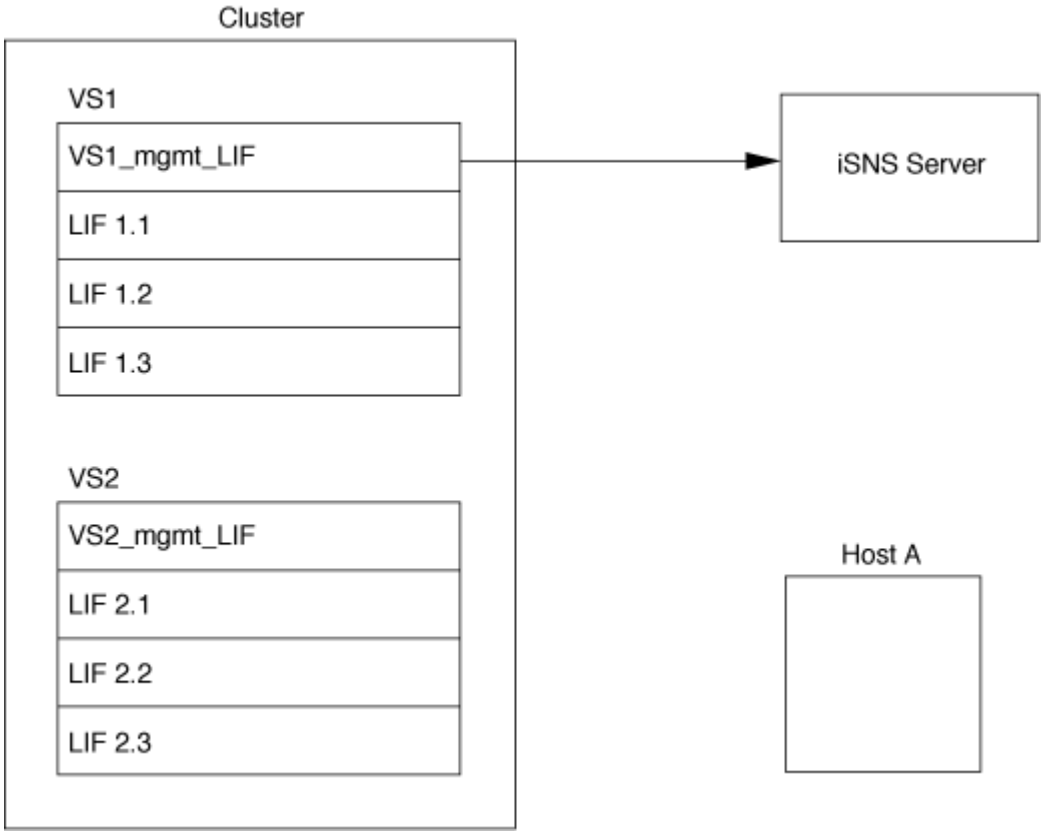
A NetApp não fornece ou revender servidores iSNS. Você pode obter esses servidores de um fornecedor suportado pelo NetApp.

Como os SVMs interagem com um servidor iSNS

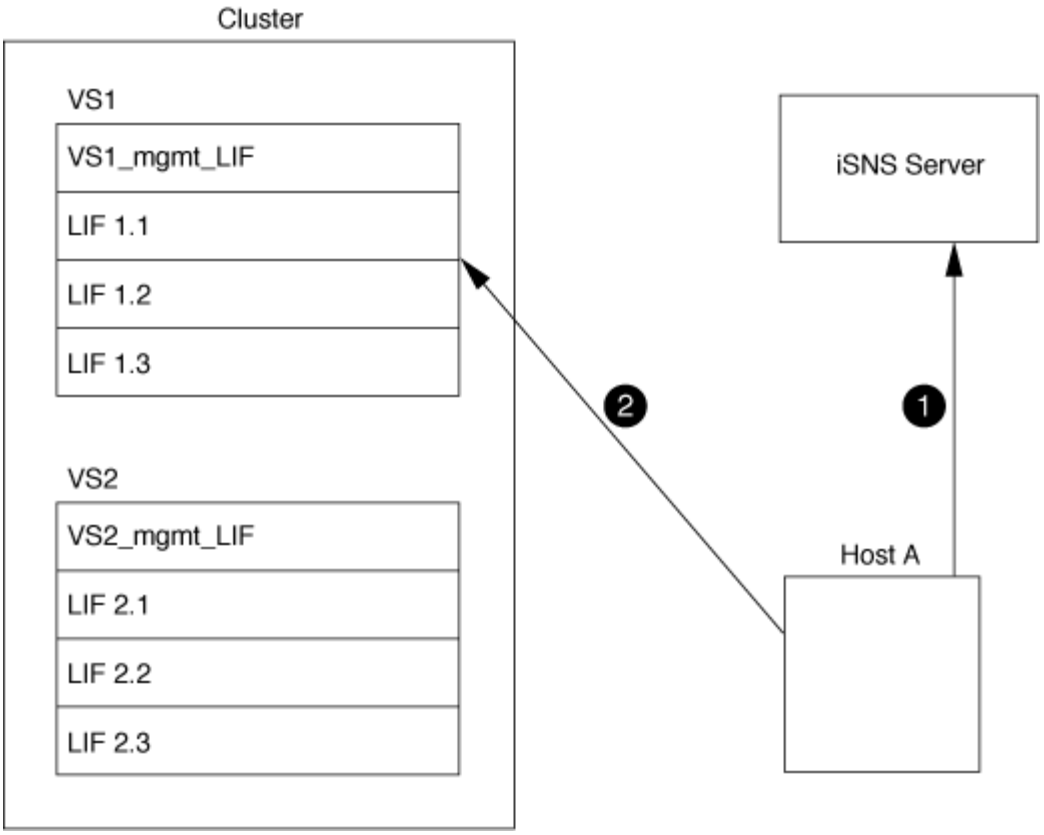
O servidor iSNS se comunica com cada máquina virtual de storage (SVM) por meio do LIF de gerenciamento do SVM. O LIF de gerenciamento Registra todos os nomes, alias e informações do portal do nó de destino iSCSI com o serviço iSNS para um SVM específico.

No exemplo a seguir, o SVM "'VS1'" usa o gerenciamento de SVM LIF "'VS1_mgmt_lif" para se Registrar no servidor iSNS. Durante o Registro do iSNS, um SVM envia todas as LIFs iSCSI por meio do LIF de gerenciamento do SVM para o iSNS Server. Depois que o Registro do iSNS for concluído, o servidor iSNS tem uma lista de todos os LIFs que servem iSCSI em "'VS1"". Se um cluster contiver vários SVMs, cada SVM

precisará se Registrar individualmente no servidor iSNS para usar o serviço iSNS.



No próximo exemplo, depois que o servidor iSNS concluir o Registro com o destino, o Host A pode descobrir todos os LIFs para "'VS1" através do servidor iSNS, conforme indicado na Etapa 1. Depois que o Host A concluir a descoberta dos LIFs para "'VS1"", o Host A pode estabelecer uma conexão com qualquer um dos LIFs em "'VS1"", como mostrado na Etapa 2. O host A não está ciente de nenhum dos LIFs em "'VS2" até que o LIF de gerenciamento "'VS2_mgmt_LIF" para Registros "'VS2" com o servidor iSNS.



No entanto, se você definir as listas de acesso à interface, o host só poderá usar as LIFs definidas na lista de acesso à interface para acessar o destino.

Depois que o iSNS for configurado inicialmente, o ONTAP atualizará automaticamente o servidor iSNS quando as configurações do SVM mudarem.

Pode ocorrer um atraso de alguns minutos entre o momento em que você faz as alterações de configuração e quando o ONTAP envia a atualização para o servidor iSNS. Forçar uma atualização imediata das informações do iSNS no servidor iSNS: `vserver iscsi isns update`

Comandos para gerenciar iSNS

O ONTAP fornece comandos para gerenciar seu serviço iSNS.

Se você quiser…	Use este comando…
Configurar um serviço iSNS	`vserver iscsi isns create`
Inicie um serviço iSNS	`vserver iscsi isns start`
Modifique um serviço iSNS	`vserver iscsi isns modify`
Exibir a configuração do serviço iSNS	`vserver iscsi isns show`
Forçar uma atualização das informações do iSNS registradas	`vserver iscsi isns update`

Pare um serviço iSNS	`vserver iscsi isns stop`
Remova um serviço iSNS	`vserver iscsi isns delete`
Veja a página de manual para um comando	`man command name`

Consulte a página de manual de cada comando para obter mais informações.

Provisionamento DE SAN com FC

Você deve estar ciente dos conceitos importantes que são necessários para entender como o ONTAP implementa uma SAN FC.

Como os nós de destino FC se conetam à rede

Os sistemas de storage e os hosts têm adaptadores para que possam ser conectados a switches FC com cabos.

Quando um nó é conetado à SAN FC, cada SVM Registra o World Wide Port Name (WWPN) de seu LIF com o switch Fabric Name Service. O WWNN do SVM e o WWPN de cada LIF é atribuído automaticamente pelo ONTAP.

> A conexão direta com nós de hosts com FC não é suportada, NPIV é necessária e isso requer que um switch seja usado. Com sessões iSCSI, a comunicação funciona com conexões roteadas ou conetadas diretamente à rede. No entanto, ambos os métodos são suportados com o ONTAP.

Como os nós FC são identificados

Cada SVM configurado com FC é identificado por um nome de nó mundial (WWNN).

Como WWPNs são usados

As WWPNs identificam cada LIF em uma SVM configurada para dar suporte ao FC. Essas LIFs utilizam as portas FC físicas em cada nó do cluster, que podem ser placas de destino FC, UTA ou UTA2 configuradas como FC ou FCoE nos nós.

- Criando um grupo de iniciadores

  Os WWPNs dos HBAs do host são usados para criar um grupo de iniciadores (iggroup). Um iggroup é usado para controlar o acesso do host a LUNs específicos. Você pode criar um grupo de iniciadores especificando uma coleção de WWPNs de iniciadores em uma rede FC. Quando você mapeia um LUN em um sistema de armazenamento para um grupo, você pode conceder a todos os iniciadores nesse grupo acesso a esse LUN. Se o WWPN de um host não estiver em um grupo que é mapeado para um LUN, esse host não terá acesso ao LUN. Isso significa que os LUNs não aparecem como discos nesse host.

  Você também pode criar conjuntos de portas para tornar um LUN visível apenas em portas de destino específicas. Um conjunto de portas consiste em um grupo de portas de destino FC. Você pode vincular um iggroup a um conjunto de portas. Qualquer host no grupo pode acessar os LUNs somente conetando-se às portas de destino no conjunto de portas.

- Identificação única de FC LIFs

  WWPNs identificam de forma exclusiva cada interface lógica FC. O sistema operacional host usa a combinação de WWNN e WWPN para identificar SVMs e FC LIFs. Alguns sistemas operacionais exigem vinculação persistente para garantir que o LUN seja exibido no mesmo ID de destino no host.

Como as atribuições de nomes em todo o mundo funcionam

Nomes mundiais são criados sequencialmente em ONTAP. No entanto, devido à forma como o ONTAP os atribui, eles podem parecer atribuídos em uma ordem não sequencial.

Cada adaptador tem um WWPN e WWNN pré-configurados, mas o ONTAP não usa esses valores pré-configurados. Em vez disso, o ONTAP atribui seus próprios WWPNs ou WWNNs, com base nos endereços MAC das portas Ethernet integradas.

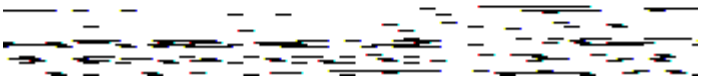
Os nomes mundiais podem parecer não sequenciais quando atribuídos pelas seguintes razões:

- Nomes mundiais são atribuídos em todos os nós e máquinas virtuais de storage (SVMs) no cluster.
- Os nomes do mundo livre são reciclados e adicionados de volta ao conjunto de nomes disponíveis.

Como os switches FC são identificados

Os switches Fibre Channel têm um nome de nó mundial (WWNN) para o próprio dispositivo e um nome de porta mundial (WWPN) para cada uma de suas portas.

Por exemplo, o diagrama a seguir mostra como os WWPNs são atribuídos a cada uma das portas em um switch Brocade de 16 portas. Para obter detalhes sobre como as portas são numeradas para um switch específico, consulte a documentação fornecida pelo fornecedor para esse switch.



Porta **0**, WWPN 20:**00**:00:60:69:51:06:B4

Porta **1**, WWPN 20:**01**:00:60:69:51:06:B4

Porta **14**, WWPN 20:**0e**:00:60:69:51:06:B4

Porta **15**, WWPN 20:**0f**:00:60:69:51:06:B4

Provisionamento DE SAN com NVMe

A partir do ONTAP 9.4, o NVMe/FC é compatível com ambiente SAN. O NVMe/FC permite que os administradores de storage provisionem namespaces e subsistemas e mapeem os namespaces para subsistemas, de forma semelhante à maneira como os LUNs são provisionados e mapeados para grupos de FC e iSCSI.

Um namespace NVMe é uma quantidade de memória não volátil que pode ser formatada em blocos lógicos. Namespaces são o equivalente a LUNs para protocolos FC e iSCSI, e um subsistema NVMe é análogo a um

iggroup. Um subsistema NVMe pode ser associado a iniciadores para que os namespaces dentro do subsistema possam ser acessados pelos iniciadores associados.

> Embora análogos em função, os namespaces NVMe não são compatíveis com todos os recursos compatíveis com LUNs.

A partir do ONTAP 9.5, é necessária uma licença para dar suporte ao acesso de dados voltado para o host com NVMe. Se o NVMe estiver habilitado no ONTAP 9.4, um período de carência de 90 dias será concedido para adquirir a licença após a atualização para o ONTAP 9.5. Se você tiver "ONTAP One", as licenças NVMe serão incluídas. Você pode ativar a licença usando o seguinte comando:

```
system license add -license-code NVMe_license_key
```

Informações relacionadas

"Relatório técnico da NetApp 4684: Implementando e configurando SANs modernas com NVMe/FC"

Volumes SAN

Sobre a visão geral dos volumes SAN

O ONTAP oferece três opções básicas de provisionamento de volume: Provisionamento thick, thin Provisioning e provisionamento semi-thick. Cada opção usa maneiras diferentes de gerenciar o espaço de volume e os requisitos de espaço para as tecnologias de compartilhamento de blocos do ONTAP. Entender como as opções funcionam permite que você escolha a melhor opção para o seu ambiente.

> Não é recomendável colocar LUNs SAN e compartilhamentos nas no mesmo FlexVol volume. Você deve provisionar volumes FlexVol separados, especificamente para suas LUNs de SAN, e provisionar volumes FlexVol separados, especificamente para seus compartilhamentos nas. Isso simplifica as implantações de gerenciamento e replicação, além de simplificar o modo como os volumes do FlexVol são suportados no Active IQ Unified Manager (anteriormente OnCommand Unified Manager).

Thin Provisioning para volumes

Quando um volume provisionado é criado, o ONTAP não reserva nenhum espaço extra quando o volume é criado. À medida que os dados são gravados no volume, o volume solicita o storage de que ele precisa do agregado para acomodar a operação de gravação. O uso de volumes provisionados por thin permite comprometer seu agregado, o que introduz a possibilidade de o volume não ser capaz de proteger o espaço necessário quando o agregado ficar sem espaço livre.

Você cria um FlexVol volume com provisionamento reduzido definindo sua `-space-guarantee` opção como `none`.

Provisionamento espesso para volumes

Quando um volume provisionado com espessura é criado, o ONTAP reserva armazenamento suficiente do agregado para garantir que qualquer bloco no volume possa ser gravado a qualquer momento. Ao configurar um volume para usar o provisionamento thick, você pode empregar qualquer um dos recursos de eficiência de storage da ONTAP, como compactação e deduplicação, para compensar os maiores requisitos de storage iniciais.

Você cria um FlexVol volume com provisionamento excessivo definindo sua `-space-slo` opção (objetivo de nível de serviço) como `thick`.

Provisionamento semi-espesso para volumes

Quando um volume usando provisionamento semi-espesso é criado, o ONTAP separa o espaço de armazenamento do agregado para contabilizar o tamanho do volume. Se o volume estiver sem espaço livre porque os blocos estão em uso por tecnologias de compartilhamento de bloco, o ONTAP se esforça para excluir objetos de dados de proteção (cópias Snapshot e arquivos FlexClone e LUNs) para liberar o espaço que eles estão segurando. Enquanto o ONTAP puder excluir os objetos de dados de proteção com a rapidez suficiente para acompanhar o espaço necessário para sobrescritas, as operações de gravação continuarão a ser bem-sucedidas. Isso é chamado de garantia de escrita "melhor esforço".

Observação: a seguinte funcionalidade não é suportada em volumes que usam provisionamento semi-espesso:

- tecnologias de eficiência de storage, como deduplicação, compressão e compactação
- Microsoft offloaded Data Transfer (ODX)

Você cria um FlexVol volume provisionado semi-espesso definindo sua `-space-slo` opção (objetivo de nível de serviço) como `semi-thick`.

Use com arquivos e LUNs reservados ao espaço

Um arquivo ou LUN com espaço reservado é aquele para o qual o armazenamento é alocado quando é criado. Historicamente, o NetApp usou o termo "LUN com provisionamento reduzido" para significar um LUN para o qual a reserva de espaço está desativada (um LUN sem espaço reservado).

*Nota: * Arquivos não reservados ao espaço não são geralmente chamados de "arquivos thin-provisionados".

A tabela a seguir resume as principais diferenças em como as três opções de provisionamento de volume podem ser usadas com arquivos reservados ao espaço e LUNs:

Provisionamento de volume	Reserva de espaço LUN/ficheiro	Sobrescreve	Proteção de dados 2	A eficiência de armazenamento 3
Espesso	Suportado	1	Garantido	Suportado
Fino	Sem efeito	Nenhum	Garantido	Suportado
Semi-espesso	Suportado	O melhor esforço 1	Melhor esforço	Não suportado

Notas

1. A capacidade de garantir substituições ou fornecer uma garantia de substituição de melhor esforço requer que a reserva de espaço esteja ativada no LUN ou arquivo.
2. Os dados de proteção incluem cópias Snapshot e arquivos FlexClone e LUNs marcados para exclusão automática (clones de backup).
3. A eficiência de storage inclui deduplicação, compactação, arquivos FlexClone e LUNs não marcados para exclusão automática (clones ativos) e subarquivos FlexClone (usados para descarregar cópias).

Suporte para LUNs de thin Provisioning SCSI

O ONTAP oferece suporte a T10 LUNs de thin Provisioning SCSI, bem como LUNs de thin Provisioning NetApp. O thin Provisioning SCSI T10 permite que os aplicativos host suportem recursos SCSI, incluindo recuperação de espaço LUN e recursos de monitoramento de espaço LUN para ambientes de blocos. O thin Provisioning SCSI T10 deve ser suportado pelo software de host SCSI.

Você usa a configuração ONTAP `space-allocation` para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 em um LUN. Você usa a configuração ONTAP `space-allocation enable` para habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

O `[-space-allocation {enabled|disabled}]` comando no Manual de Referência de comando do ONTAP tem mais informações para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 e habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

"Referência do comando ONTAP"

Configurar opções de provisionamento de volume

Você pode configurar um volume para thin Provisioning, thin Provisioning ou provisionamento semi-espesso.

Sobre esta tarefa

Definir a `-space-slo` opção para `thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- 100% do espaço necessário para as substituições é reservado. Você não pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`

Definir a `-space-slo` opção para `semi-thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- Nenhum espaço é reservado para substituições. Você pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`.
- A exclusão automática de cópias Snapshot está ativada.

Passo

1. Configurar opções de provisionamento de volume:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   A `-space-guarantee` opção padrão é `none` para sistemas AFF e para volumes DP não AFF. Caso contrário, o padrão é `volume`. Para volumes FlexVol existentes, use o `volume modify` comando para configurar opções de provisionamento.

   O comando a seguir configura o vol1 no SVM VS1 para thin Provisioning:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
none
```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento espesso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento semi-espesso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
thick
```

Opções de configuração de VOLUME SAN

Tem de definir várias opções no volume que contém o LUN. A forma como definir as opções de volume determina a quantidade de espaço disponível para LUNs no volume.

Crescimento automático

Você pode ativar ou desativar o crescimento automático. Se você ativá-lo, o crescimento automático permite que o ONTAP aumente automaticamente o tamanho do volume até um tamanho máximo que você predeterminar. Deve haver espaço disponível no agregado contendo para suportar o crescimento automático do volume. Portanto, se você ativar o crescimento automático, você deve monitorar o espaço livre no agregado contendo e adicionar mais quando necessário.

O crescimento automático não pode ser acionado para suportar a criação de Snapshot. Se você tentar criar uma cópia Snapshot e não houver espaço suficiente no volume, a criação de snapshot falhará, mesmo com o crescimento automático ativado.

Se o crescimento automático estiver desativado, o tamanho do seu volume permanecerá o mesmo.

Auto-retrátil

Pode ativar ou desativar o Autoshink. Se você ativá-lo, o recurso de auto-redução permite que o ONTAP diminua automaticamente o tamanho geral de um volume quando a quantidade de espaço consumida no volume diminui um limite predeterminado. Isso aumenta a eficiência de storage acionando volumes para liberar espaço livre não utilizado automaticamente.

snapshot Autodelete

O snapshot autodelete exclui automaticamente cópias snapshot quando uma das seguintes situações ocorre:

- O volume está quase cheio.
- O espaço de reserva do Snapshot está quase cheio.
- O espaço de reserva de substituição está cheio.

Você pode configurar o snapshot autodelete para excluir cópias Snapshot do mais antigo para o mais recente

ou do mais recente para o mais antigo. O snapshot autodelete não exclui cópias snapshot vinculadas a cópias snapshot em volumes clonados ou LUNs.

Se o seu volume precisar de espaço adicional e você tiver ativado o crescimento automático e o snapshot Autodelete, por padrão, o ONTAP tentará adquirir o espaço necessário acionando primeiro o crescimento automático. Se não for adquirido espaço suficiente através do crescimento automático, o snapshot autodelete é acionado.

Reserva do Snapshot

A reserva do Snapshot define a quantidade de espaço no volume reservado para cópias Snapshot. O espaço alocado à reserva Instantânea não pode ser usado para qualquer outra finalidade. Se todo o espaço alocado para o Snapshot Reserve for usado, as cópias Snapshot começarão a consumir espaço adicional no volume.

Requisito para movimentação de volumes em ambientes SAN

Antes de mover um volume que contenha LUNs ou namespaces, você precisa atender a certos requisitos.

- Para volumes que contêm um ou mais LUNs, você deve ter no mínimo dois caminhos por LUN (LIFs) conetados a cada nó no cluster.

  Isso elimina pontos únicos de falha e permite que o sistema sobreviva a falhas de componentes.

- Para volumes que contêm namespaces, o cluster precisa estar executando o ONTAP 9.6 ou posterior.

  A movimentação de volume não é compatível com configurações NVMe que executam o ONTAP 9.5.

Considerações para definir a reserva fracionária

A reserva fracionária, também chamada de *reserva de substituição LUN*, permite desativar a reserva de substituição para LUNs e arquivos reservados no espaço em um FlexVol volume. Isso pode ajudar a maximizar a utilização do storage, mas se o ambiente for afetado negativamente por falhas nas operações de gravação devido à falta de espaço, você precisa entender os requisitos que essa configuração impõe.

A configuração de reserva fracionária é expressa como uma porcentagem; os únicos valores válidos são `0` e `100` porcentagem. A configuração de reserva fracionária é um atributo do volume.

Definir a reserva fracionária para `0` aumentar a utilização do armazenamento. No entanto, um aplicativo que acessa dados que residem no volume pode ter uma interrupção de dados se o volume estiver sem espaço livre, mesmo com a garantia de volume definida como `volume`. No entanto, com a configuração e o uso adequados de volume, você pode minimizar a chance de falhas de gravação. O ONTAP fornece uma garantia de gravação "melhor esforço" para volumes com reserva fracionária definida para `0` quando *todos* dos seguintes requisitos são atendidos:

- A deduplicação não está em uso
- A compressão não está a ser utilizada
- Os subficheiros FlexClone não estão a ser utilizados
- Todos os arquivos FlexClone e LUNs FlexClone são ativados para exclusão automática

Esta não é a configuração padrão. Você deve ativar explicitamente a exclusão automática, seja no momento da criação ou modificando o arquivo FlexClone ou LUN FlexClone depois que ele for criado.

- A descarga de cópia ODX e FlexClone não está em uso
- A garantia de volume está definida para `volume`
- A reserva de espaço de arquivo ou LUN é `enabled`
- A reserva de instantâneo de volume está definida como `0`
- A exclusão automática da cópia Snapshot do volume é `enabled` com um nível de compromisso de `destroy`, uma lista de destruição de `lun_clone,vol_clone,cifs_share,file_clone,sfsr` e um gatilho de `volume`

  Essa configuração também garante que arquivos FlexClone e LUNs FlexClone sejam excluídos quando necessário.

Observe que, se sua taxa de alteração for alta, em casos raros, a exclusão automática da cópia Snapshot pode ficar para trás, resultando em falta de espaço no volume, mesmo com todas as configurações necessárias acima em uso.

Além disso, você pode, como opção, usar a funcionalidade de volume com crescimento automático para diminuir a probabilidade de as cópias do Snapshot precisarem ser excluídas automaticamente. Se você ativar a capacidade de crescimento automático, deverá monitorar o espaço livre no agregado associado. Se o agregado ficar cheio o suficiente para que o volume seja impedido de crescer, mais cópias Snapshot provavelmente serão excluídas à medida que o espaço livre no volume estiver esgotado.

Se você não puder atender a todos os requisitos de configuração acima e precisar garantir que o volume não fique sem espaço, defina a configuração de reserva fracionária do volume como `100`. Isso requer mais espaço livre na frente, mas garante que as operações de modificação de dados serão bem-sucedidas mesmo quando as tecnologias listadas acima estiverem em uso.

O valor padrão e os valores permitidos para a configuração de reserva fracionária dependem da garantia do volume:

Garantia de volume	Reserva fracionária predefinida	Valores permitidos
Volume	100	0, 100
Nenhum	0	0, 100

Gerenciamento de espaço no lado do host SAN

Em um ambiente com provisionamento reduzido, o gerenciamento de espaço no lado do host conclui o processo de gerenciamento de espaço do sistema de storage que foi liberado no sistema de arquivos do host.

Um sistema de arquivos host contém metadados para acompanhar quais blocos estão disponíveis para armazenar novos dados e quais blocos contêm dados válidos que não devem ser sobrescritos. Esses metadados são armazenados no LUN ou namespace. Quando um arquivo é excluído no sistema de arquivos host, os metadados do sistema de arquivos são atualizados para marcar os blocos desse arquivo como espaço livre. O espaço livre total do sistema de arquivos é então recalculado para incluir os blocos recém-liberados. Para o sistema de storage, essas atualizações de metadados não parecem diferentes de quaisquer

outras gravações que estejam sendo executadas pelo host. Portanto, o sistema de armazenamento não tem conhecimento de que quaisquer exclusões ocorreram.

Isso cria uma discrepância entre a quantidade de espaço livre relatada pelo host e a quantidade de espaço livre relatada pelo sistema de armazenamento subjacente. Por exemplo, suponha que você tenha um LUN de 200 GB recém-provisionado atribuído ao seu host pelo sistema de armazenamento. Tanto o host quanto o sistema de armazenamento relatam 200 GB de espaço livre. Seu host então grava 100 GB de dados. Nesse ponto, tanto o host quanto o sistema de armazenamento relatam 100 GB de espaço usado e 100 GB de espaço não utilizado.

Em seguida, você exclui 50 GB de dados do seu host. Neste ponto, seu host irá relatar 50 GB de espaço usado e 150 GB de espaço não utilizado. No entanto, seu sistema de armazenamento irá relatar 100 GB de espaço usado e 100 GB de espaço não utilizado.

O gerenciamento de espaço no lado do host usa vários métodos para reconciliar o diferencial de espaço entre o host e o sistema de armazenamento.

Gerenciamento de host simplificado com o SnapCenter

Você pode usar o software SnapCenter para simplificar algumas tarefas de gerenciamento e proteção de dados associadas ao storage iSCSI e FC. O SnapCenter é um pacote de gerenciamento opcional para hosts Windows e UNIX.

Você pode usar o software SnapCenter para criar facilmente discos virtuais de pools de storage que podem ser distribuídos entre vários sistemas de storage e automatizar as tarefas de provisionamento de storage e simplificar o processo de criação de cópias Snapshot e clones consistentes com os dados de host.

Consulte a documentação do produto NetApp para obter mais informações "SnapCenter" sobre .

Links relacionados

"Ativar a alocação de espaço ONTAP para protocolos SAN"

Sobre os grupos

Grupos de iniciadores (grupos de iniciadores) são tabelas de WWPNs de host de protocolo FC ou nomes de nós de host iSCSI. Você pode definir grupos e mapeá-los para LUNs para controlar quais iniciadores têm acesso a LUNs.

Normalmente, você deseja que todas as portas de iniciador do host ou iniciadores de software tenham acesso a um LUN. Se você estiver usando software multipathing ou tiver hosts em cluster, cada porta iniciador ou iniciador de software de cada host em cluster precisa de caminhos redundantes para o mesmo LUN.

Você pode criar grupos que especificam quais iniciadores têm acesso aos LUNs antes ou depois de criar LUNs, mas você deve criar grupos antes de poder mapear um LUN para um grupo.

Os grupos de iniciadores podem ter vários iniciadores, e vários grupos podem ter o mesmo iniciador. No entanto, não é possível mapear um LUN para vários grupos que tenham o mesmo iniciador. Um iniciador não pode ser um membro de grupos de diferentes ostypes.

Exemplo de como os grupos dão acesso LUN

Você pode criar vários grupos para definir quais LUNs estão disponíveis para seus hosts. Por exemplo, se você tiver um cluster de host, pode usar igroups para garantir que LUNs específicos sejam visíveis para apenas um host no cluster ou para todos os hosts no cluster.

A tabela a seguir ilustra como quatro grupos dão acesso aos LUNs para quatro hosts diferentes que estão acessando o sistema de armazenamento. Os hosts em cluster (Host3 e Host4) são membros do mesmo grupo (Group3) e podem acessar os LUNs mapeados para esse grupo. O grupo chamado Group4 contém as WWPNs de Host4 para armazenar informações locais que não se destinam a ser vistas por seu parceiro.

Hosts com WWPNs HBA, IQNs ou EUIs	grupos	WWPNs, IQNs, EUIs adicionados aos grupos	LUNs mapeados para grupos
Host1, caminho único (iniciador de software iSCSI) iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2, multipath (dois HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3, multipath, em cluster com host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
Host4, multipath, agrupado (não visível para Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Especifique WWPNs do iniciador e nomes de nó iSCSI para um grupo

Você pode especificar os nomes de nós iSCSI e WWPNs dos iniciadores quando você cria um iggroup ou pode adicioná-los mais tarde. Se você optar por especificar os nomes dos nós iSCSI do iniciador e WWPNs ao criar o LUN, eles poderão ser removidos mais tarde, se necessário.

Siga as instruções na documentação dos Utilitários de host para obter WWPNs e localizar os nomes de nó iSCSI associados a um host específico. Para hosts que executam o software ESX, use o Virtual Storage Console.

Virtualização de storage com descarga de cópia VMware e Microsoft

Visão geral da virtualização de storage com descarga de cópia VMware e Microsoft

VMware e Microsoft suportam operações de descarga de cópia para aumentar o desempenho e a taxa de transferência de rede. Você deve configurar o sistema para atender aos requisitos dos ambientes do sistema operacional VMware e Windows para usar suas respetivas funções de descarga de cópia.

Ao usar a descarga de cópia da VMware e da Microsoft em ambientes virtualizados, os LUNs precisam estar alinhados. LUNs desalinhados podem degradar o desempenho.

Vantagens de usar um ambiente SAN virtualizado

A criação de um ambiente virtualizado com o uso de máquinas virtuais de storage (SVMs) e LIFs permite expandir seu ambiente SAN para todos os nós do cluster.

- Gerenciamento distribuído

  É possível fazer login em qualquer nó da SVM para administrar todos os nós em um cluster.

- Maior acesso aos dados

  Com o MPIO e o ALUA, você tem acesso aos dados por meio de iSCSI ou FC LIFs ativos para o SVM.

- Acesso controlado LUN

  Se você usar SLM e portsets, poderá limitar quais LIFs um iniciador pode usar para acessar LUNs.

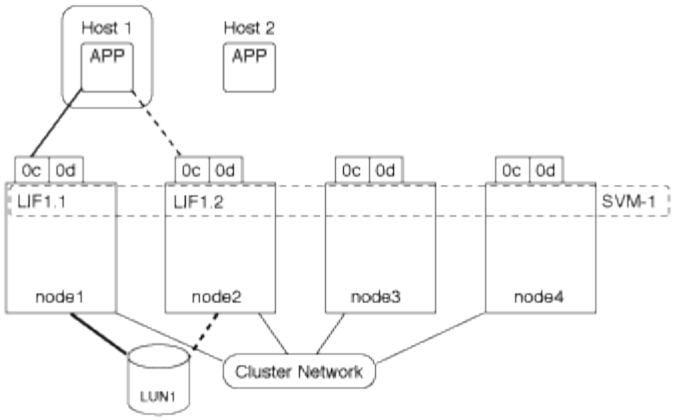
Como o acesso LUN funciona em um ambiente virtualizado

Em um ambiente virtualizado, os LIFs permitem que os hosts (clientes) acessem LUNs por meio de caminhos otimizados e não otimizados.

Um LIF é uma interface lógica que coneta o SVM a uma porta física. Embora vários SVMs possam ter várias LIFs na mesma porta, um LIF pertence a uma SVM. Você pode acessar LUNs por meio das LIFs SVMs.

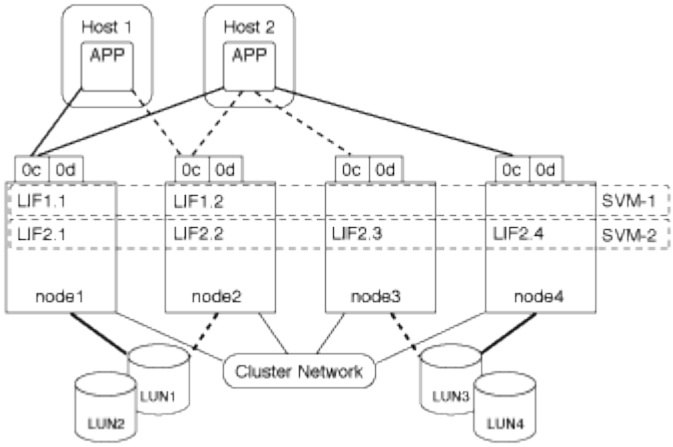
Exemplo de acesso LUN com uma única SVM em um cluster

No exemplo a seguir, o host 1 se conecta ao LIF1,1 e LIF1,2 no SVM-1 para acessar o LUN1. LIF1,1 usa a porta física node1:0C e LIF1,2 usa o node2:0C. O LIF1,1 e o LIF1,2 pertencem apenas à SVM-1. Se um novo LUN for criado no nó 1 ou no nó 2, para SVM-1, ele poderá usar essas mesmas LIFs. Se um novo SVM for criado, novas LIFs poderão ser criadas usando as portas físicas 0C ou 0d em ambos os nós.



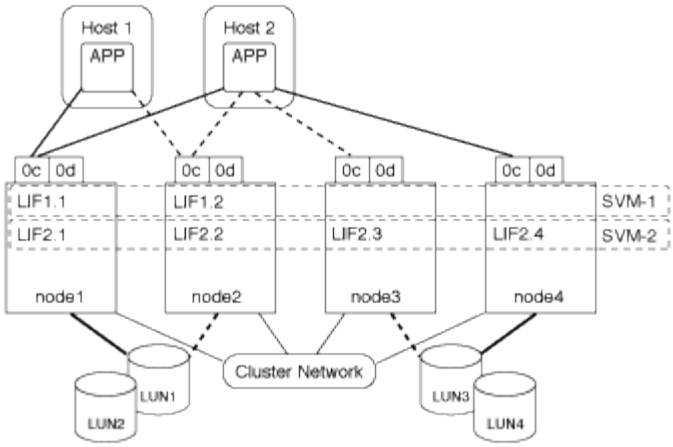
Exemplo de acesso LUN com vários SVMs em um cluster

Uma porta física pode suportar vários LIFs que servem diferentes SVMs. Como os LIFs estão associados a uma SVM específica, os nós de cluster podem enviar o tráfego de dados de entrada para o SVM correto. No exemplo a seguir, cada nó de 1 a 4 tem um LIF para SVM-2 usando a porta física 0C em cada nó. O host 1 se conecta ao LIF1,1 e ao LIF1,2 na SVM-1 para acessar o LUN1. O host 2 se conecta ao LIF2-1 e ao LIF2-2 na SVM-2 para acessar o LUN2. Ambos os SVMs estão compartilhando a porta física 0C nos nós 1 e 2. O SVM-2 tem LIFs adicionais que o host 2 está usando para acessar LUNs 3 e 4. Esses LIFs estão usando a porta física 0C nos nós 3 e 4. Vários SVMs podem compartilhar as portas físicas nos nós.



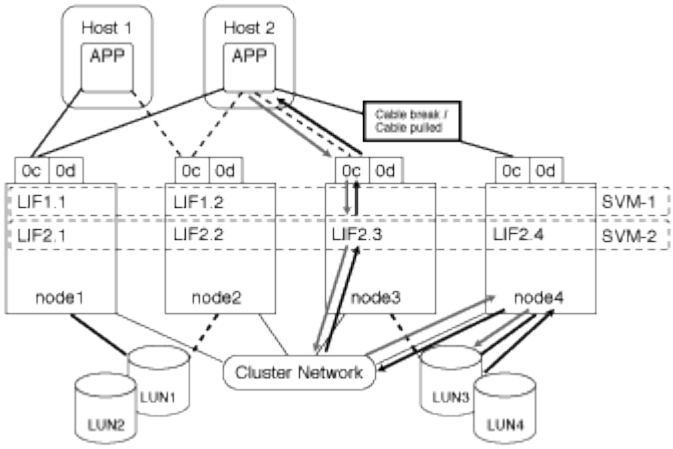
Exemplo de um caminho ativo ou otimizado para um LUN a partir de um sistema host

Em um caminho ativo ou otimizado, o tráfego de dados não percorre a rede do cluster; ele viaja a rota mais direta para o LUN. O caminho ativo ou otimizado para LUN1 é através de LIF1,1 em node1, usando a porta física 0C. O host 2 tem dois caminhos ativos ou otimizados, um caminho para node1, LIF2,1, que está compartilhando a porta física 0C e o outro caminho para node4, LIF2,4, que está usando a porta física 0C.



Exemplo de um caminho ativo ou não otimizado (indireto) para um LUN a partir de um sistema host

Em um caminho ativo ou não otimizado (indireto), o tráfego de dados viaja pela rede do cluster. Esse problema ocorre somente se todos os caminhos ativos ou otimizados de um host não estiverem disponíveis para lidar com o tráfego. Se o caminho do Host 2 para o SVM-2 LIF2,4 for perdido, o acesso ao LUN3 e ao LUN4 percorre a rede do cluster. O acesso a partir do Host 2 usa o LIF2,3 em node3. Em seguida, o tráfego entra no switch de rede do cluster e faz backup de até node4 para acesso ao LUN3 e ao LUN4. Em seguida, ele passará para trás pelo switch de rede de cluster e, em seguida, voltará para o LIF2,3 para o Host 2. Esse caminho ativo ou não otimizado é usado até que o caminho para o LIF2,4 seja restaurado ou um novo LIF seja estabelecido para SVM-2 em outra porta física no nó 4.



=
:allow-uri-read:

Melhorar o desempenho do VMware VAAI para hosts ESX

O ONTAP oferece suporte a determinados recursos de VMware vStorage APIs para integração de storage (VAAI) quando o host ESX estiver executando o ESX 4,1 ou posterior. Esses recursos ajudam a descarregar as operações do host ESX para o sistema de storage e a aumentar a taxa de transferência da rede. O host ESX habilita os recursos automaticamente no ambiente correto.

O recurso VAAI suporta os seguintes comandos SCSI:

- `EXTENDED_COPY`

Esse recurso permite que o host inicie a transferência de dados entre os LUNs ou em um LUN sem envolver o host na transferência de dados. Isso resulta em salvar ciclos de CPU ESX e aumentar a taxa de transferência da rede. O recurso de cópia estendida, também conhecido como "descarga de cópia", é usado em cenários como clonagem de uma máquina virtual. Quando invocado pelo host ESX, o recurso de descarga de cópia copia os dados dentro do sistema de storage em vez de passar pela rede do host. A descarga de cópia transfere dados das seguintes maneiras:

  - Dentro de um LUN
  - Entre LUNs em um volume
  - Entre LUNs em diferentes volumes em uma máquina virtual de storage (SVM)
  - Entre LUNs em diferentes SVMs dentro de um cluster se esse recurso não puder ser invocado, o host ESX usa automaticamente os comandos padrão DE LEITURA e GRAVAÇÃO para a operação de cópia.

- `WRITE_SAME`

  Esse recurso descarrega o trabalho de escrever um padrão repetido, como todos os zeros, para um storage array. O host ESX usa esse recurso em operações como o preenchimento zero de um arquivo.

- `COMPARE_AND_WRITE`

  Esse recurso ignora certos limites de simultaneidade de acesso a arquivos, o que acelera operações como inicializar máquinas virtuais.

Requisitos para usar o ambiente VAAI

Os recursos VAAI fazem parte do sistema operacional ESX e são invocados automaticamente pelo host ESX quando você configurou o ambiente correto.

Os requisitos ambientais são os seguintes:

- O host ESX deve estar executando o ESX 4,1 ou posterior.
- O sistema de storage NetApp que hospeda o armazenamento de dados VMware deve estar executando o ONTAP.
- (Somente descarga de cópia) a origem e o destino da operação de cópia VMware devem ser hospedados no mesmo sistema de storage no mesmo cluster.

> O recurso de descarga de cópia atualmente não oferece suporte à cópia de dados entre datastores VMware hospedados em diferentes sistemas de storage.

Determine se os recursos VAAI são suportados pelo ESX

Para confirmar se o sistema operacional ESX suporta os recursos VAAI, você pode verificar o vSphere Client ou usar qualquer outro meio de acessar o host. O ONTAP suporta os comandos SCSI por padrão.

Você pode verificar as configurações avançadas do host ESX para determinar se os recursos do VAAI estão ativados. A tabela indica quais comandos SCSI correspondem aos nomes de controle ESX.

Comando SCSI	Nome do controle ESX (recurso VAAI)
EXTENDED_COPY (CÓPIA_ESTENDIDA)	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
COMPARE_E_ESCREVA	`HardwareAcceleratedLocking`

Microsoft offloaded Data Transfer (ODX)

A Microsoft Offloaded Data Transfer (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro de um dispositivo de armazenamento ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host.

O ONTAP oferece suporte ao ODX para os protocolos SMB e SAN.

Em transferências de arquivos não ODX, os dados são lidos da origem e são transferidos pela rede para o host. O host transfere os dados de volta pela rede para o destino. Na transferência de arquivos ODX, os dados são copiados diretamente da origem para o destino sem passar pelo host.

Como as cópias descarregadas do ODX são executadas diretamente entre a origem e o destino, benefícios significativos de desempenho são obtidos se as cópias forem executadas dentro do mesmo volume, incluindo tempo de cópia mais rápido para cópias do mesmo volume, utilização reduzida da CPU e memória no cliente e utilização reduzida da largura de banda de e/S de rede. Se as cópias estiverem em volumes, talvez não haja ganhos significativos de desempenho em comparação com as cópias baseadas em host.

Para ambientes SAN, o ODX só está disponível quando é suportado pelo host e pelo sistema de armazenamento. Os computadores clientes que suportam ODX e têm o ODX ativado automaticamente e de forma transparente usam transferência de arquivos descarregados ao mover ou copiar arquivos. O ODX é usado independentemente de você arrastar e soltar arquivos através do Windows Explorer ou usar comandos de cópia de arquivo de linha de comando ou se um aplicativo cliente inicia solicitações de cópia de arquivo.

Requisitos para usar ODX

Se você planeja usar o ODX para descarregamentos de cópias, você precisa estar familiarizado com considerações de suporte de volume, requisitos de sistema e requisitos de capacidade de software.

Para usar o ODX, seu sistema deve ter o seguinte:

- ONTAP

  O ODX é ativado automaticamente em versões suportadas do ONTAP.

- Volume mínimo de origem de 2 GB

  Para um desempenho ideal, o volume de origem deve ser superior a 260 GB.

- Suporte ODX no cliente Windows

  O ODX é suportado no Windows Server 2012 ou posterior e no Windows 8 ou posterior. A Matriz de interoperabilidade contém as informações mais recentes sobre clientes Windows suportados.

"Ferramenta de Matriz de interoperabilidade do NetApp"

- Cópia de suporte de aplicativo para ODX

  O aplicativo que executa a transferência de dados deve suportar ODX. As operações de aplicação que suportam ODX incluem o seguinte:

  - Operações de gerenciamento do Hyper-V, como criar e converter discos rígidos virtuais (VHDs), gerenciar cópias Snapshot e copiar arquivos entre máquinas virtuais
  - Operações do Windows Explorer
  - Comandos de cópia do Windows PowerShell
  - Comandos de cópia do prompt de comando do Windows a Biblioteca Microsoft TechNet contém mais informações sobre aplicativos ODX suportados em servidores e clientes Windows.
- Se você usar volumes compatados, o tamanho do grupo de compactação deve ser 8K.

  O tamanho do grupo de compressão 32K não é suportado.

O ODX não funciona com os seguintes tipos de volume:

- Volumes de origem com capacidades inferiores a 2 GB
- Volumes só de leitura
- "Volumes FlexCache"

  O ODX é compatível com volumes de origem FlexCache.
- "Volumes provisionados semi-grossos"

Requisitos especiais de arquivo do sistema

Você pode excluir arquivos ODX encontrados no qtrees. Você não deve remover ou modificar quaisquer outros arquivos de sistema ODX, a menos que você seja informado pelo suporte técnico para fazê-lo.

Ao usar o recurso ODX, existem arquivos de sistema ODX que existem em cada volume do sistema. Esses arquivos permitem a representação pontual dos dados usados durante a transferência do ODX. Os seguintes arquivos de sistema estão no nível raiz de cada volume que contém LUNs ou arquivos para os quais os dados foram descarregados:

- `.copy-offload` (um diretório oculto)
- `.tokens` (arquivo sob o diretório oculto `.copy-offload`)

Você pode usar o `copy-offload delete-tokens -path dir_path -node` *`node_name`* comando para excluir uma qtree contendo um arquivo ODX.

Casos de uso para ODX

Você deve estar ciente dos casos de uso para usar o ODX em SVMs para que você possa determinar em que circunstâncias o ODX fornece benefícios de desempenho.

Os servidores e clientes do Windows que suportam ODX usam a descarga de cópia como a forma padrão de copiar dados em servidores remotos. Se o servidor ou cliente do Windows não suportar ODX ou a descarga de cópia ODX falhar em qualquer ponto, a operação de cópia ou movimentação volta para leituras e

gravações tradicionais para a operação de cópia ou movimentação.

Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

- Inter-cluster

  As LUNs de origem e destino estão em volumes diferentes, localizados em nós diferentes, entre clusters. Isso só é suportado para SAN e não funciona para SMB.

Existem alguns casos de uso especiais adicionais:

- Com a implementação do ONTAP ODX, você pode usar o ODX para copiar arquivos entre compartilhamentos SMB e unidades virtuais conetadas a FC ou iSCSI.

  Você pode usar o Windows Explorer, a CLI do Windows ou PowerShell, Hyper-V ou outras aplicações compatíveis com ODX para copiar ou mover arquivos sem interrupções usando a descarga de cópia ODX entre compartilhamentos SMB e LUNs conetados, desde que os compartilhamentos SMB e LUNs estejam no mesmo cluster.

- O Hyper-V fornece alguns casos de uso adicionais para descarga de cópia ODX:

  - Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

    Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

  - Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
  - A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Administração da SAN

Provisionamento DE SAN

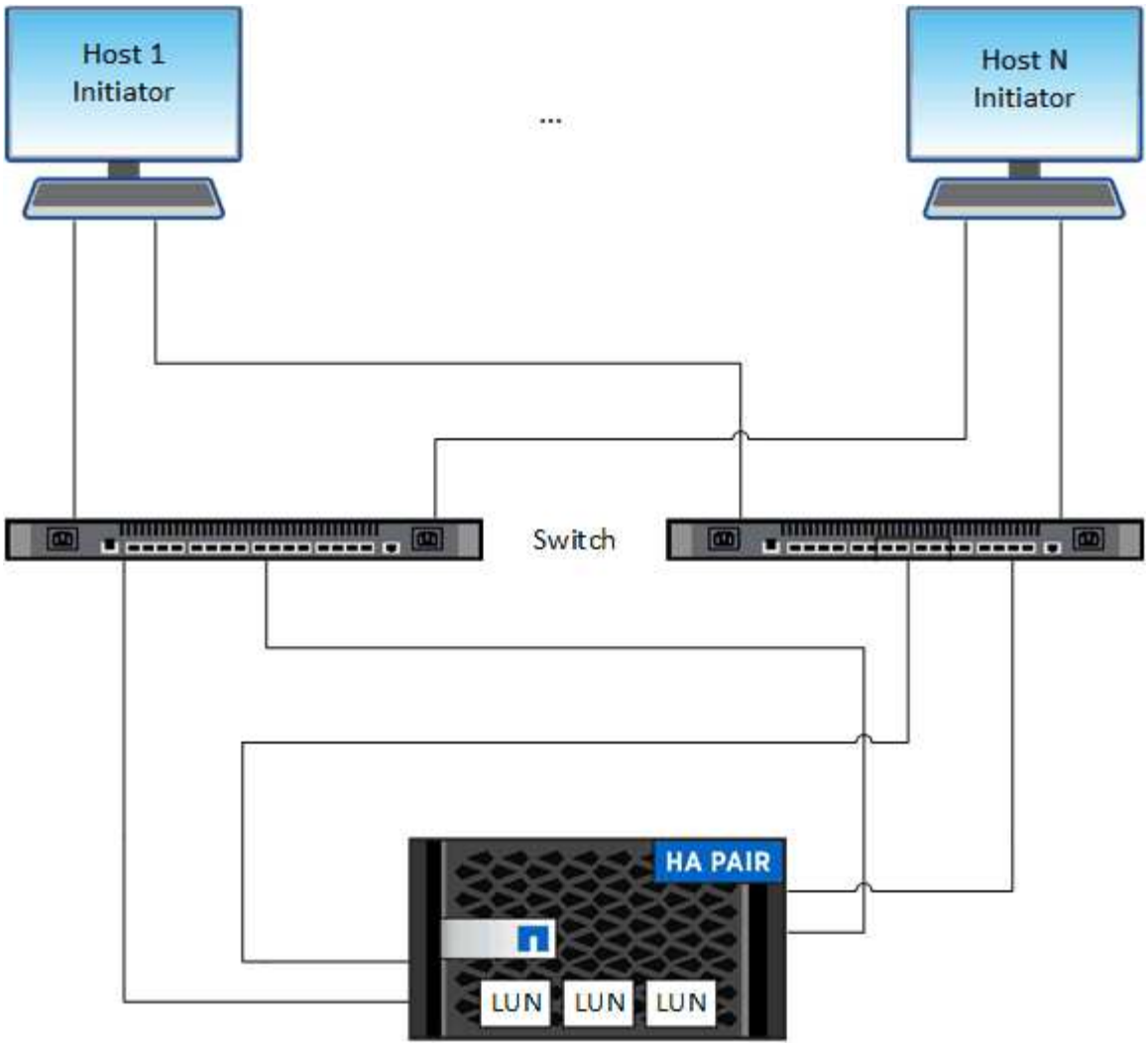
Visão geral do gerenciamento DE SAN

O conteúdo desta seção mostra como configurar e gerenciar ambientes SAN com a interface de linha de comando (CLI) do ONTAP e o Gerenciador de sistemas no ONTAP 9.7 e versões posteriores.

Se você estiver usando o gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), consulte estes tópicos:

- "Protocolo iSCSI"
- "Protocolo FC/FCoE"

Você pode usar os protocolos iSCSI e FC para fornecer storage em um ambiente SAN.



Com iSCSI e FC, os destinos de armazenamento são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Você cria LUNs e, em seguida, mapeia-os para grupos de iniciadores (grupos de iniciadores). Grupos de iniciadores são tabelas de WWPs de host FC e nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs.

Os destinos FC se conetam à rede por meio de switches FC e adaptadores do lado do host e são identificados por nomes de portas mundiais (WWPNs). Os destinos iSCSI se conetam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs).

Para mais informações

Se você tiver um sistema de storage ASA R2 (ASA A1K, ASA A70, ASA A90), consulte "Documentação do sistema de storage ASA R2".

Configurar switches para FCoE

Você deve configurar seus switches para FCoE antes que seu serviço FC possa ser executado sobre a infraestrutura Ethernet existente.

O que você vai precisar

- Sua configuração SAN precisa ser compatível.

Para obter mais informações sobre as configurações suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

- Um adaptador de destino unificado (UTA) deve ser instalado em seu sistema de armazenamento.

  Se você estiver usando um UTA2, ele deve ser definido para `cna` o modo.

- Um adaptador de rede convergente (CNA) deve ser instalado em seu host.

Passos

1. Use a documentação do switch para configurar os switches para FCoE.
2. Verifique se as configurações do DCB para cada nó no cluster foram configuradas corretamente.

   ```
   run -node node1 -command dcb show
   ```

   As definições do DCB são configuradas no interrutor. Consulte a documentação do switch se as configurações estiverem incorretas.

3. Verifique se o login FCoE está funcionando quando o status on-line da porta de destino FC for `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   Se o status on-line da porta de destino FC for `false`, consulte a documentação do switch.

Informações relacionadas

- "Ferramenta de Matriz de interoperabilidade do NetApp"
- "Relatório técnico da NetApp 3800: Guia de implantação completa em Fibre Channel over Ethernet (FCoE)"
- "Guias de configuração de software Cisco MDS 9000 NX-os e SAN-os"
- "Produtos Brocade"

Requisitos do sistema

A configuração de LUNs envolve a criação de um LUN, a criação de um grupo e o mapeamento do LUN para o grupo. O sistema deve atender a certos pré-requisitos antes de configurar os LUNs.

- A Matriz de interoperabilidade deve listar sua configuração de SAN como suportada.
- Seu ambiente SAN precisa atender aos limites de configuração de controladora e host SAN especificados na "NetApp Hardware Universe" para sua versão do software ONTAP.
- É necessário instalar uma versão suportada dos Utilitários do sistema anfitrião.

  A documentação Host Utilities (Utilitários do host) fornece mais informações.

- Você precisa ter SAN LIFs no nó proprietário do LUN e no parceiro de HA do nó proprietário.

Informações relacionadas

- "Ferramenta de Matriz de interoperabilidade do NetApp"
- "Configuração do host SAN ONTAP"
- "Relatório técnico da NetApp 4017: Práticas recomendadas de SAN Fibre Channel"

O que saber antes de criar um LUN

Por que os tamanhos reais de LUN variam ligeiramente

Você deve estar ciente do seguinte em relação ao tamanho de seus LUNs.

- Quando você cria um LUN , o tamanho real do LUN pode variar ligeiramente com base no tipo de SO do LUN. O tipo de SO LUN não pode ser modificado após a criação do LUN.
- Se você criar um LUN no tamanho máximo de LUN, esteja ciente de que o tamanho real do LUN pode ser um pouco menor. ONTAP arredonda o limite para ser um pouco menos.
- Os metadados para cada LUN requerem aproximadamente 64 KB de espaço no agregado que contém. Ao criar um LUN, você deve garantir que o agregado que contém tenha espaço suficiente para os metadados do LUN. Se o agregado não contiver espaço suficiente para os metadados do LUN, alguns hosts poderão não conseguir acessar o LUN.

Diretrizes para a atribuição de IDs de LUN

Normalmente, o ID de LUN padrão começa com 0 e é atribuído em incrementos de 1 para cada LUN mapeado adicional. O host associa a ID LUN com o local e o nome do caminho do LUN. O intervalo de números de ID LUN válidos depende do host. Para obter informações detalhadas, consulte a documentação fornecida com seus Utilitários de host.

Diretrizes para mapeamento de LUNs para grupos

- Você pode mapear um LUN apenas uma vez para um grupo.
- Como prática recomendada, você deve mapear um LUN para apenas um iniciador específico através do grupo.
- Você pode adicionar um único iniciador a vários grupos, mas o iniciador pode ser mapeado para apenas um LUN.
- Não é possível usar o mesmo ID de LUN para dois LUNs mapeados para o mesmo grupo.
- Você deve usar o mesmo tipo de protocolo para grupos e conjuntos de portas.

Verifique e adicione sua licença de protocolo FC ou iSCSI

Antes de habilitar o acesso a bloco de uma máquina virtual de storage (SVM) com FC ou iSCSI, você precisa ter uma licença. As licenças FC e iSCSI estão incluídas no "ONTAP One".

Exemplo 11. Passos

System Manager

Se você não tiver o ONTAP One, verifique e adicione sua licença FC ou iSCSI com o Gerenciador de sistema do ONTAP (9,7 e posterior).

1. No System Manager, selecione **Cluster > Settings > Licenses**
2. Se a licença não estiver listada, + Add selecione e insira a chave de licença.
3. Selecione **Adicionar**.

CLI

Se você não tiver o ONTAP One, verifique e adicione sua licença FC ou iSCSI com a CLI do ONTAP.

1. Verifique se você tem uma licença ativa para FC ou iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- --------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Se não tiver uma licença ativa para FC ou iSCSI, adicione o seu código de licença.

```
license add -license-code <your_license_code>
```

Provisionamento de storage SAN

Esse procedimento cria novos LUNs em uma VM de storage existente que já tenha o protocolo FC ou iSCSI configurado.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para provisionar seu storage. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Se for necessário criar uma nova VM de storage e configurar o protocolo FC ou iSCSI, consulte "Configurar um SVM para FC" ou "Configurar um SVM para iSCSI".

Se a licença FC não estiver ativada, os LIFs e SVMs parecem estar online, mas o status operacional está

inativo.

Os LUNs aparecem no seu host como dispositivos de disco.

> O acesso de unidade lógica assimétrica (ALUA) é sempre ativado durante a criação de LUN. Não é possível alterar a definição ALUA.

Você deve usar o zoneamento de iniciador único para todos os LIFs FC no SVM para hospedar os iniciadores.

A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.

Exemplo 12. Passos

System Manager

Criar LUNs para fornecer storage para um host SAN usando o protocolo FC ou iSCSI com o Gerenciador de sistemas ONTAP (9,7 e posterior).

Para concluir esta tarefa utilizando o System Manager Classic (disponível com 9,7 e anterior), consulte "Configuração iSCSI para Red Hat Enterprise Linux"

Passos

1. Instale o apropriado "Utilitários de host SAN" em seu host.
2. No System Manager, clique em **Storage > LUNs** e, em seguida, clique em **Add**.
3. Introduza as informações necessárias para criar o LUN.
4. Você pode clicar em **mais Opções** para fazer qualquer uma das seguintes opções, dependendo da sua versão do ONTAP.

Opção	Disponível a partir de
• Atribuir política de QoS a LUNs em vez de volume pai ◦ **Mais Opções > armazenamento e Otimização** ◦ Selecione **nível de serviço de desempenho**. ◦ Para aplicar a política de QoS a LUNs individuais em vez de todo o volume, selecione **aplicar esses limites de desempenho a cada LUN**. Por padrão, os limites de desempenho são aplicados ao nível do volume.	ONTAP 9.10,1
• Crie um novo grupo de iniciadores usando grupos de iniciadores existentes ◦ **Mais Opções > INFORMAÇÕES DO HOST** ◦ Selecione **novo grupo de iniciadores usando grupos de iniciadores existentes**. ⓘ O tipo de sistema operacional para um grupo contendo outros grupos não pode ser alterado depois que ele foi criado.	ONTAP 9.9,1
• Adicione uma descrição ao seu grupo ou iniciador do host A descrição serve como um alias para o igroup ou iniciador do host. ◦ **Mais Opções > INFORMAÇÕES DO HOST**	ONTAP 9.9,1

• Crie seu LUN em um volume existente Por padrão, um novo LUN é criado em um novo volume. ◦ **Mais Opções > Adicionar LUNs** ◦ Selecione **Group Related LUNs**.	ONTAP 9.9,1
• Desative a QoS ou escolha uma política de QoS personalizada ◦ **Mais Opções > armazenamento e Otimização** ◦ Selecione **nível de serviço de desempenho**. No ONTAP 9.9,1 e posterior, se você selecionar uma política de QoS personalizada, também poderá selecionar posicionamento manual em um nível local especificado.	ONTAP 9,8

5. Para FC, coloque a zona dos seus comutadores FC pela WWPN. Use uma zona por iniciador e inclua todas as portas de destino em cada zona.
6. Descubra LUNs no seu host.

   Para o VMware vSphere, use o Virtual Storage Console (VSC) para descobrir e inicializar seus LUNs.
7. Inicialize os LUNs e, opcionalmente, crie sistemas de arquivos.
8. Verifique se o host pode gravar e ler dados no LUN.

CLI

Crie LUNs para fornecer storage para um host SAN usando o protocolo FC ou iSCSI com a CLI do ONTAP.

1. Verifique se você tem uma licença para FC ou iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Se você não tiver uma licença para FC ou iSCSI, use o `license add` comando.

```
license add -license-code <your_license_code>
```

3. Habilite o serviço de protocolos no SVM:

   Para iSCSI:

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   Para FC:

   ```
   vserver fcp create -vserver <svm_name> -status-admin up
   ```

4. Crie duas LIFs para as SVMs em cada nó:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   O NetApp é compatível com, no mínimo, um iSCSI ou FC LIF por nó para cada SVM que fornece dados. No entanto, dois LIFS por nó são necessários para redundância. Para iSCSI, é recomendável configurar um mínimo de duas LIFs por nó em redes Ethernet separadas.

5. Verifique se seus LIFs foram criados e se o status operacional deles é `online`:

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. Crie seus LUNs:

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   O seu nome LUN não pode exceder 255 carateres e não pode conter espaços.

   ⓘ A opção NVFAIL é ativada automaticamente quando um LUN é criado em um volume.

7. Crie seus grupos:

   ```
   igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
   <fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
   ```

8. Mapeie seus LUNs para grupos:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Verifique se os LUNs estão configurados corretamente:

```
lun show -vserver <svm_name>
```

10. Opcionalmente"Crie um conjunto de portas e vincule a um grupo", .
11. Siga as etapas na documentação do host para habilitar o acesso a blocos em seus hosts específicos.
12. Use os Utilitários do host para concluir o mapeamento FC ou iSCSI e descobrir os LUNs no host.

Informações relacionadas

- "Visão geral da administração DE SAN"
- "Configuração do host SAN ONTAP"
- "Exibir e gerenciar grupos de iniciadores SAN no System Manager"
- "Relatório técnico da NetApp 4017: Práticas recomendadas de SAN Fibre Channel"

Provisionamento NVMe

Visão geral do NVMe

Você pode usar o protocolo NVMe (non-volátil Memory Express) para fornecer storage em um ambiente SAN. O protocolo NVMe é otimizado para performance com storage de estado sólido.

Para NVMe, os destinos de storage são chamados de namespaces. Um namespace NVMe é uma quantidade de storage não volátil que pode ser formatada em blocos lógicos e apresentada a um host como um dispositivo de bloco padrão. Você cria namespaces e subsistemas e, em seguida, mapeia os namespaces para os subsistemas, semelhante à maneira como os LUNs são provisionados e mapeados para grupos para FC e iSCSI.

Os destinos NVMe são conectados à rede por meio de uma infraestrutura FC padrão usando switches FC ou uma infraestrutura TCP padrão usando switches Ethernet e adaptadores no lado do host.

O suporte a NVMe varia de acordo com a sua versão do ONTAP. "Limitações e suporte do NVMe"Consulte para obter detalhes.

O que é NVMe

O protocolo não volátil Memory Express (NVMe) é um protocolo de transporte usado para acessar Mídia de storage não volátil.

O NVMe sobre Fabrics (NVMeoF) é uma extensão definida por especificação do NVMe que permite a comunicação baseada em NVMe por conexões que não PCIe. Esta interface permite que gabinetes de armazenamento externos sejam conetados a um servidor.

O NVMe foi desenvolvido para fornecer acesso eficiente a dispositivos de storage criados com memória não

volátil, da tecnologia flash às tecnologias de memória persistente e de alta performance. Como tal, ele não tem as mesmas limitações que os protocolos de armazenamento projetados para unidades de disco rígido. Os dispositivos flash e de estado sólido (SSDs) são um tipo de memória não volátil (NVM). NVM é um tipo de memória que mantém seu conteúdo durante uma queda de energia. O NVMe é uma maneira de acessar essa memória.

Os benefícios do NVMe incluem maiores velocidades, produtividade, taxa de transferência e capacidade para transferência de dados. As caraterísticas específicas incluem o seguinte:

- O NVMe foi projetado para ter até 64 mil filas.

  Cada fila, por sua vez, pode ter até 64 mil comandos simultâneos.

- O NVMe é compatível com vários fornecedores de hardware e software
- O NMVe é mais produtivo com as tecnologias Flash que permitem tempos de resposta mais rápidos
- O NVMe permite várias solicitações de dados para cada "demanda" enviada para o SSD.

  O NVMe leva menos tempo para decodificar um "request" e não requer bloqueio de threads em um programa multithread.

- O NVMe oferece suporte a funcionalidades que impedem a perda de peso no nível da CPU e permitem escalabilidade massiva à medida que os sistemas se expandem.

Sobre os namespaces NVMe

Um namespace NVMe é uma quantidade de memória não volátil (NVM) que pode ser formatada em blocos lógicos. Namespaces são usados quando uma máquina virtual de storage é configurada com o protocolo NVMe e são equivalentes a LUNs para protocolos FC e iSCSI.

Um ou mais namespaces são provisionados e conectados a um host NVMe. Cada namespace pode suportar vários tamanhos de bloco.

O protocolo NVMe fornece acesso a namespaces por meio de várias controladoras. Usando drivers NVMe, que são compatíveis com a maioria dos sistemas operacionais, os namespaces de unidade de estado sólido (SSD) aparecem como dispositivos de bloco padrão nos quais sistemas de arquivos e aplicativos podem ser implantados sem qualquer modificação.

Um ID de namespace (NSID) é um identificador usado por um controlador para fornecer acesso a um namespace. Ao definir o NSID para um host ou grupo de hosts, você também configura a acessibilidade a um volume por um host. Um bloco lógico só pode ser mapeado para um único grupo de host de cada vez, e um determinado grupo de host não tem NSIDs duplicados.

Sobre os subsistemas NVMe

Um subsistema NVMe inclui uma ou mais controladores NVMe, namespaces, portas de subsistema NVM, um meio de storage NVM e uma interface entre a controladora e o meio de storage NVM. Quando você cria um namespace NVMe, por padrão ele não é mapeado para um subsistema. Você também pode optar por mapear um subsistema novo ou existente.

Informações relacionadas

- Aprenda a "Provisionamento de storage NVMe" usar os sistemas ASA, AFF e FAS
- Saiba mais sobre "Mapear um namespace NVMe para um subsistema"os sistemas ASA AFF e FAS.
- "Configurar hosts SAN e clientes em nuvem"

- Aprenda a "Provisionamento de storage SAN" usar os sistemas de armazenamento ASA R2 (ASA A1K, ASA A70 ou ASA A90).

Requisitos de licença NVMe

A partir do ONTAP 9.5, é necessária uma licença para dar suporte ao NVMe. Se o NVMe estiver habilitado no ONTAP 9.4, um período de carência de 90 dias será concedido para adquirir a licença após a atualização para o ONTAP 9.5.

Você pode ativar a licença usando o seguinte comando:

```
system license add -license-code NVMe_license_key
```

Configuração, suporte e limitações do NVMe

A partir do ONTAP 9.4, o "Memória expressa (NVMe) não volátil" protocolo está disponível para ambientes SAN. O FC-NVMe usa a mesma configuração física e prática de zoneamento das redes FC tradicionais, mas permite maior largura de banda, IOPs maiores e latência reduzida do que o FC-SCSI.

As limitações e o suporte do NVMe variam de acordo com a versão do ONTAP, a plataforma e a configuração. Para obter detalhes sobre sua configuração específica, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter os limites suportados, "Hardware Universe"consulte .

> O máximo de nós por cluster está disponível no Hardware Universe em **mistura de plataformas suportadas**.

Configuração

- É possível configurar a configuração NVMe usando uma única malha ou várias malhas.
- Você deve configurar um LIF de gerenciamento para cada SVM que suporte SAN.
- O uso de malhas de switch FC heterogêneas não é suportado, exceto no caso de switches blade incorporados.

  Exceções específicas estão listadas no "Ferramenta de Matriz de interoperabilidade do NetApp".

- Cascata, malha parcial, malha completa, borda central e tecidos diretor são todos métodos padrão do setor de conexão de switches FC a uma malha e todos são compatíveis.

  Uma malha pode consistir em um ou vários switches, e os controladores de storage podem ser conectados a vários switches.

Caraterísticas

Os recursos NVMe a seguir são compatíveis com base na sua versão do ONTAP.

Começando com ONTAP…	Compatível com NVMe
9.15.1	• Configurações de IP MetroCluster de quatro nós em NVMe/TCP

9.14.1	• Definir a prioridade do host no subsistema (QoS em nível de host)
9.12.1	• Configurações de IP MetroCluster de quatro nós no NVMe/FC • As configurações do MetroCluster não são compatíveis com redes NVMe front-end anteriores ao ONTAP 9.12,1. • As configurações do MetroCluster não são compatíveis com NVMe/TCP.
9.10.1	Redimensionamento de um namespace
9.9.1	• Coexistência de namespaces e LUNs no mesmo volume
9,8	• Coexistência do protocolo Os protocolos SCSI, nas e NVMe podem existir na mesma máquina virtual de storage (SVM). Antes do ONTAP 9.8, o NVMe pode ser o único protocolo na SVM.
9,6	• blocos de 512 bytes e blocos de 4096 bytes para namespaces 4096 é o valor padrão. 512 só deve ser usado se o sistema operacional host não suportar blocos de 4096 bytes. • Movimentação de volume com namespaces mapeados
9,5	• Failover de par de HA multipath/giveback

Protocolos

Os protocolos NVMe a seguir são compatíveis.

Protocolo	Começando com ONTAP…	Permitido por…
TCP	9.10.1	Padrão
FC	9,4	Padrão

A partir do ONTAP 9.8, é possível configurar protocolos SCSI, nas e NVMe na mesma máquina virtual de storage (SVM). No ONTAP 9.7 e versões anteriores, o NVMe pode ser o único protocolo na SVM.

Namespaces

Ao trabalhar com namespaces NVMe, você deve estar ciente do seguinte:

- O ONTAP não é compatível com o comando NVMe dataset Management (desalocar) com o NVMe para exigência de espaço.
- Não é possível usar o SnapRestore para restaurar um namespace de um LUN ou vice-versa.
- A garantia de espaço para namespaces é a mesma que a garantia de espaço do volume contendo.
- Não é possível criar um namespace em uma transição de volume do Data ONTAP operando no modo 7D.
- Namespaces não suportam o seguinte:
  - Renomeação
  - Movimento entre volumes
  - Cópia entre volumes
  - Cópia sob demanda

Limitações adicionais

Os seguintes recursos do ONTAP não são compatíveis com configurações NVMe:

- Sincronização ativa do SnapMirror
- Console de armazenamento virtual
- Reservas persistentes

O seguinte aplica-se apenas aos nós que executam o ONTAP 9.4:

- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- O serviço NVMe deve ser criado antes da criação do NVMe LIF.

Informações relacionadas

"Práticas recomendadas para SAN moderna"

Configurar uma VM de storage para NVMe

Para usar o protocolo NVMe em um nó, configure o SVM especificamente para NVMe.

Antes de começar

Seus adaptadores FC ou Ethernet devem ser compatíveis com NVMe. Os adaptadores suportados estão listados no "NetApp Hardware Universe".

Exemplo 13. Passos

System Manager

Configurar uma VM de storage para NVMe com o ONTAP System Manager (9,7 e posterior).

Para configurar o NVMe em uma nova VM de storage	Para configurar o NVMe em uma VM de storage existente
1. No System Manager, clique em **Storage > Storage VMs** e, em seguida, clique em **Add**. 2. Introduza um nome para a VM de armazenamento. 3. Selecione **NVMe** para o **Access Protocol**. 4. Selecione **Ativar NVMe/FC** ou **Ativar NVMe/TCP** e **Salvar**.	1. No System Manager, clique em **Storage > Storage VMs**. 2. Clique na VM de armazenamento que você deseja configurar. 3. Clique na guia **Configurações** e, em seguida, clique ⚙ ao lado do protocolo NVMe. 4. Selecione **Ativar NVMe/FC** ou **Ativar NVMe/TCP** e **Salvar**.

CLI

Configurar uma VM de storage para NVMe com a CLI do ONTAP.

1. Se você não quiser usar um SVM existente, crie um:

```
vserver create -vserver <SVM_name>
```

   a. Verifique se o SVM foi criado:

```
vserver show
```

2. Verifique se você tem adaptadores compatíveis com NVMe ou TCP instalados no cluster:

   Para NVMe:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   Para TCP:

```
network port show
```

3. Se você estiver executando o ONTAP 9.7 ou anterior, remova todos os protocolos do SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

A partir do ONTAP 9.8, não é necessário remover outros protocolos ao adicionar o NVMe.

4. Adicionar o protocolo NVMe à SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Se você estiver executando o ONTAP 9.7 ou anterior, verifique se o NVMe é o único protocolo permitido no SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

O NVMe deve ser o único protocolo exibido sob a `allowed protocols` coluna.

6. Criar o serviço NVMe:

```
vserver nvme create -vserver <SVM_name>
```

7. Verifique se o serviço NVMe foi criado:

```
vserver nvme show -vserver <SVM_name>
```

O `Administrative Status` do SVM deve ser listado como `up`.

8. Criar um LIF NVMe/FC:
   - Para ONTAP 9.9,1 ou anterior, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -role data -data
-protocol fc-nvme -home-node <home_node> -home-port <home_port>
```

   - Para ONTAP 9.10,1 ou posterior, FC ou TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp | default-data-nvme-fc> -data-protocol
<fcp | fc-nvme | nvme-tcp> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

9. Crie um NVMe/FC LIF no nó de parceiro de HA:

- Para ONTAP 9.9,1 ou anterior, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- Para ONTAP 9.10,1 ou posterior, FC ou TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. Verifique se os LIFs NVMe/FC foram criados:

```
network interface show -vserver <SVM_name>
```

11. Criar volume no mesmo nó que o LIF:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Se for apresentada uma mensagem de aviso sobre a política de eficiência automática, esta pode ser ignorada com segurança.

Provisionamento de storage NVMe

Use estas etapas para criar namespaces e provisionar storage para qualquer host compatível com NVMe em uma VM de storage existente.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para provisionar seu storage. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.

Antes de começar

Sua VM de storage deve estar configurada para NVMe, e seu transporte FC ou TCP já deve estar configurado.

System Manager

Usando o Gerenciador de sistemas do ONTAP (9,7 e posterior), crie namespaces para fornecer storage usando o protocolo NVMe.

Passos

1. No System Manager, clique em **Storage > NVMe Namespaces** e, em seguida, clique em **Add**.

   Se precisar criar um novo subsistema, clique em **mais Opções**.

2. Se você estiver executando o ONTAP 9.8 ou posterior e quiser desativar o QoS ou escolher uma política de QoS personalizada, clique em **mais opções** e, em **armazenamento e otimização**, selecione **nível de serviço de desempenho**.
3. Coloque as suas centrais FC por WWPN. Use uma zona por iniciador e inclua todas as portas de destino em cada zona.
4. No seu host, descubra os novos namespaces.
5. Inicialize o namespace e formate-o com um sistema de arquivos.
6. Verifique se o host pode gravar e ler dados no namespace.

CLI

Com a CLI do ONTAP, crie namespaces para fornecer storage usando o protocolo NVMe.

Esse procedimento cria um namespace e um subsistema NVMe em uma VM de storage existente que já foi configurada para o protocolo NVMe e, em seguida, mapeia o namespace para o subsistema para permitir acesso a dados do sistema host.

Se precisar configurar a VM de storage para NVMe, "Configurar um SVM para NVMe"consulte .

Passos

1. Verifique se o SVM está configurado para NVMe:

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` deve ser exibido sob a `allowed-protocols` coluna.

2. Crie o namespace NVMe:

   > O volume que você faz referência com o `-path` parâmetro já deve existir ou você precisará criar um antes de executar este comando.

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. Crie o subsistema NVMe:

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

O nome do subsistema NVMe diferencia maiúsculas de minúsculas. Deve conter 1 a 96 carateres. Carateres especiais são permitidos.

4. Verifique se o subsistema foi criado:

```
vserver nvme subsystem show -vserver <svm_name>
```

O `nvme` subsistema deve ser exibido sob a `Subsystem` coluna.

5. Obtenha o NQN do host.
6. Adicione o NQN do host ao subsistema:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. Mapeie o namespace para o subsistema:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

Um namespace só pode ser mapeado para um único subsistema.

8. Verifique se o namespace está mapeado para o subsistema:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

O subsistema deve ser listado como `Attached subsystem` .

Mapear um namespace NVMe para um subsistema

O mapeamento de um namespace NVMe para um subsistema permite acesso aos dados do seu host. É possível mapear um namespace NVMe para um subsistema quando você provisiona o storage ou pode fazê-lo depois que o storage tiver sido provisionado.

A partir do ONTAP 9.14,1, você pode priorizar a alocação de recursos para hosts específicos. Por padrão, quando um host é adicionado ao subsistema NVMe, ele recebe prioridade regular. Você pode usar a interface de linha de comando (CLI) do ONTAP para alterar manualmente a prioridade padrão de regular para alta. Os hosts atribuídos a uma alta prioridade são alocadas contagens de filas de e/S maiores e profundidades de

filas.

Se você quiser dar uma alta prioridade a um host que foi adicionado a um subsistema no ONTAP 9.13,1 ou anterior, você pode altere a prioridade do host.

Antes de começar

Seu namespace e subsistema já devem ser criados. Se precisar criar um namespace e um subsistema, "Provisionamento de storage NVMe"consulte .

Passos

1. Obtenha o NQN do host.
2. Adicione o NQN do host ao subsistema:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

Se você quiser alterar a prioridade padrão do host de regular para alta, use a `-priority high` opção. Esta opção está disponível a partir de ONTAP 9.14,1.

3. Mapeie o namespace para o subsistema:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

Um namespace só pode ser mapeado para um único subsistema.

4. Verifique se o namespace está mapeado para o subsistema:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

O subsistema deve ser listado como `Attached subsystem` .

Gerenciar LUNs

Editar grupo de políticas de QoS LUN

A partir do ONTAP 9.10,1, você pode usar o Gerenciador de sistema para atribuir ou remover políticas de qualidade do serviço (QoS) em vários LUNs ao mesmo tempo.

Se a política de QoS for atribuída ao nível do volume, ela deverá ser alterada no nível do volume. Você só pode editar a política de QoS no nível LUN se ela foi originalmente atribuída no nível LUN.

Passos

1. No System Manager, clique em **Storage > LUNs**.

2. Selecione o LUN ou LUNs que pretende editar.

   Se você estiver editando mais de um LUN de cada vez, os LUNs devem pertencer à mesma Máquina Virtual de Storage (SVM). Se você selecionar LUNs que não pertençam ao mesmo SVM, a opção de editar o Grupo de políticas de QoS não será exibida.

3. Clique em **mais** e selecione **Editar Grupo de políticas de QoS**.

Converta um LUN em um namespace

A partir do ONTAP 9.11,1, você pode usar a CLI do ONTAP para converter no local um LUN existente em um namespace NVMe.

Antes de começar

- LUN especificado não deve ter nenhum mapa existente para um grupo.
- O LUN não deve estar em um SVM configurado pelo MetroCluster ou em uma relação de sincronização ativa do SnapMirror.
- O LUN não deve ser um endpoint de protocolo ou vinculado a um endpoint de protocolo.
- O LUN não deve ter um prefixo e/ou fluxo de sufixo não zero.
- O LUN não deve fazer parte de um instantâneo ou no lado de destino da relação do SnapMirror como um LUN somente leitura.

Passo

1. Converter um LUN para um namespace NVMe:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

Tire um LUN off-line

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para colocar LUNs off-line. Antes do ONTAP 9.10,1, você deve usar a CLI do ONTAP para colocar LUNs off-line.

System Manager

Passos

1. No System Manager, clique em **Storage>LUNs**.
2. Coloque um único LUN ou vários LUNs offline

Se você quiser…	Faça isso…
Tire um único LUN off-line	Ao lado do nome do LUN, clique ⋮ e selecione **Take Offline**.
Coloque vários LUNs offline	1. Selecione os LUNs que pretende colocar offline. 2. Clique em **More** e selecione **Take Offline**.

CLI

Você só pode colocar um LUN off-line de cada vez ao usar a CLI.

Passo

1. Coloque o LUN offline:

```
lun offline <lun_name> -vserver <SVM_name>
```

Redimensione um LUN no ONTAP

Pode aumentar ou diminuir o tamanho de um LUN.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para aumentar o tamanho de uma unidade de armazenamento. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

ⓘ Os LUNs Solaris não podem ser redimensionados.

Aumente o tamanho de um LUN

O tamanho para o qual você pode aumentar seu LUN varia dependendo da sua versão do ONTAP.

Versão de ONTAP	Tamanho máximo de LUN
ONTAP 9.12.1P2 e posterior	128 TB para plataformas AFF, FAS e ASA

ONTAP 9 F.8 e mais tarde	• 128 TB para plataformas All-Flash SAN Array (ASA) • 16 TB para plataformas não ASA
ONTAP 9.5, 9,6, 9,7	16 TB
ONTAP 9 .4 ou anterior	10 vezes o tamanho original do LUN, mas não superior a 16TB, que é o tamanho máximo do LUN. Por exemplo, se você criar um LUN de 100 GB, só poderá aumentá-lo para 1.000 GB. O tamanho máximo real do LUN pode não ser exatamente 16TB. ONTAP arredonda o limite para ser um pouco menos.

Você não precisa colocar o LUN off-line para aumentar o tamanho. No entanto, depois de aumentar o tamanho, você deve redigitalizar o LUN no host para que o host reconheça a alteração de tamanho.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//lun-resize.html[`lun resize` na referência de comando ONTAP.

Exemplo 14. Passos

System Manager

Aumente o tamanho de um LUN com o ONTAP System Manager (9,7 e posterior).

1. No System Manager, clique em **Storage > LUNs**.
2. Clique ⋮ e selecione **Editar**.
3. Em **armazenamento e Otimização** aumente o tamanho do LUN e **Salvar**.

CLI

Aumente o tamanho de um LUN com a CLI do ONTAP.

1. Aumente o tamanho do LUN:

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. Verifique o tamanho de LUN aumentado:

```
lun show -vserver <SVM_name>
```

As operações de ONTAP resumem o tamanho máximo real do LUN para que ele seja ligeiramente menor do que o valor esperado. Além disso, o tamanho real do LUN pode variar ligeiramente com base no tipo de SO do LUN. Para obter o valor exato redimensionado, execute os seguintes comandos no modo avançado:

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. Volte a digitalizar o LUN no host.
2. Siga a documentação do host para tornar o tamanho LUN recém-criado visível para o sistema de arquivos do host.

Diminua o tamanho de um LUN

Antes de diminuir o tamanho de um LUN, o host precisa migrar os blocos que contêm os dados de LUN para o limite do tamanho de LUN menor. Você deve usar uma ferramenta como o SnapCenter para garantir que o LUN seja diminuído corretamente sem truncar blocos contendo dados de LUN. Diminuir manualmente o tamanho do LUN não é recomendado.

Depois de diminuir o tamanho do LUN, o ONTAP notifica automaticamente o iniciador de que o tamanho do LUN diminuiu. No entanto, podem ser necessárias etapas adicionais no seu host para que o host reconheça o novo tamanho de LUN. Verifique a documentação do host para obter informações específicas sobre como diminuir o tamanho da estrutura do arquivo host.

Mover um LUN

Você pode mover um LUN entre volumes em uma máquina virtual de storage (SVM), mas não pode mover um LUN entre SVMs. As LUNs migradas em volumes dentro de uma SVM são movidas imediatamente e sem perda de conectividade.

O que você vai precisar

Se o LUN estiver usando o mapa de LUN seletivo (SLM), você deve "Modifique a lista de nós de relatórios SLM"incluir o nó de destino e seu parceiro de HA antes de mover o LUN.

Sobre esta tarefa

Os recursos de eficiência de storage, como deduplicação, compressão e compactação, não são preservados durante a movimentação de LUN. Eles devem ser reaplicados depois que a movimentação de LUN for concluída.

A proteção de dados com cópias Snapshot ocorre no nível do volume. Portanto, quando você move um LUN, ele se enquadra no esquema de proteção de dados do volume de destino. Se você não tiver cópias Snapshot estabelecidas para o volume de destino, as cópias Snapshot do LUN não serão criadas. Além disso, todas as cópias Snapshot do LUN permanecem no volume original até que essas cópias snapshot sejam excluídas.

Não é possível mover um LUN para os seguintes volumes:

- Um volume de destino SnapMirror
- Volume raiz do SVM

Não é possível mover os seguintes tipos de LUNs:

- Um LUN que foi criado a partir de um ficheiro
- Um LUN que está no estado NVFail
- Um LUN que está em um relacionamento de compartilhamento de carga
- Um LUN de classe de endpoint de protocolo

Para LUNs Solaris os_type que tenham 1 TB ou mais, o host pode ter um tempo limite durante a movimentação de LUN. Para esse tipo de LUN, você deve desmontar o LUN antes de iniciar a movimentação.

Exemplo 15. Passos

System Manager

Mova um LUN com o Gerenciador de sistema do ONTAP (9,7 e posterior).

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para criar um novo volume ao mover um único LUN. No ONTAP 9 1 e 9,9.8, o volume para o qual você está movendo seu LUN deve existir antes de iniciar a movimentação do LUN.

Passos

1. No System Manager, clique em **Storage>LUNs**.
2. Clique com o botão direito do rato no LUN que pretende mover e, em seguida, clique ⋮ em **mover LUN**.

   No ONTAP 9.10,1, selecione para mover o LUN para **um volume existente** ou para um **novo volume**.

   Se você selecionar para criar um novo volume, forneça as especificações de volume.
3. Clique em **mover**.

CLI

Mova um LUN com a CLI do ONTAP.

1. Mover o LUN:

   ```
   lun move start
   ```

   Durante um período muito breve, o LUN é visível tanto no volume de origem como no de destino. Isso é esperado e é resolvido após a conclusão da mudança.
2. Acompanhe o status da movimentação e verifique a conclusão bem-sucedida:

   ```
   lun move show
   ```

Informações relacionadas

- "Mapa LUN seletivo"

Eliminar LUNs

Você pode excluir um LUN de uma máquina virtual de storage (SVM) se não precisar mais do LUN.

O que você vai precisar

O LUN deve ser desmapeado do seu grupo antes de poder excluí-lo.

Passos

1. Verifique se o aplicativo ou o host não está usando o LUN.
2. Desmapeie o LUN do grupo:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. Eliminar o LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Verifique se você excluiu o LUN:

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

O que saber antes de copiar LUNs

Você deve estar ciente de certas coisas antes de copiar um LUN.

Os administradores de cluster podem copiar um LUN entre máquinas virtuais de armazenamento (SVMs) dentro do cluster usando o `lun copy` comando. Os administradores de cluster devem estabelecer a relação de peering de máquina virtual de storage (SVM) usando o comando antes de uma operação de cópia LUN entre SVM `vserver peer create` ser executada. Deve haver espaço suficiente no volume de origem para um clone SIS.

LUNs nas cópias Snapshot podem ser usadas como LUNs de origem para o `lun copy` comando. Quando você copia um LUN usando o `lun copy` comando, a cópia LUN fica imediatamente disponível para acesso de leitura e gravação. O LUN de origem não é alterado pela criação de uma cópia LUN. Tanto o LUN de origem como a cópia LUN existem como LUNs exclusivos com números de série LUN diferentes. As alterações feitas no LUN de origem não são refletidas na cópia LUN e as alterações feitas na cópia LUN não são refletidas no LUN de origem. O mapeamento LUN do LUN de origem não é copiado para o novo LUN; a cópia LUN deve ser mapeada.

A proteção de dados com cópias Snapshot ocorre no nível do volume. Portanto, se você copiar um LUN para um volume diferente do volume do LUN de origem, o LUN de destino estará sob o esquema de proteção de dados do volume de destino. Se você não tiver cópias Snapshot estabelecidas para o volume de destino, as cópias Snapshot não serão criadas da cópia LUN.

Copiar LUNs é uma operação sem interrupções.

Não é possível copiar os seguintes tipos de LUNs:

- Um LUN que foi criado a partir de um ficheiro
- Um LUN que está no estado NVFAIL
- Um LUN que está em um relacionamento de compartilhamento de carga
- Um LUN de classe de endpoint de protocolo

Examine o espaço configurado e usado de um LUN

Conhecer o espaço configurado e o espaço real usado para os LUNs pode ajudá-lo a determinar a quantidade de espaço que pode ser recuperado ao fazer a recuperação de espaço, a quantidade de espaço reservado que contém dados e o tamanho total configurado em relação ao tamanho real usado para um LUN.

Passo

1. Exibir o espaço configurado versus o espaço real usado para um LUN:

   ```
   lun show
   ```

   O exemplo a seguir mostra o espaço configurado versus o espaço real usado pelas LUNs na máquina virtual de storage (SVM) VS3:

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- ------------------      ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

Controle e monitore o desempenho de e/S para LUNs com o uso do QoS de storage

Você pode controlar a performance de entrada/saída (e/S) a LUNs atribuindo LUNs a grupos de políticas QoS de storage. Você pode controlar a performance de e/S para garantir que os workloads atinjam objetivos de performance específicos ou para controlar um workload que afeta negativamente outros workloads.

Sobre esta tarefa

Os grupos de políticas aplicam um limite máximo de taxa de transferência (por exemplo, 100 MB/s). Você pode criar um grupo de políticas sem especificar uma taxa de transferência máxima, que permite monitorar o desempenho antes de controlar a carga de trabalho.

Também é possível atribuir máquinas virtuais de storage (SVMs) a volumes e LUNs do FlexVol a grupos de políticas.

Observe os seguintes requisitos sobre a atribuição de um LUN a um grupo de políticas:

- O LUN deve estar contido pelo SVM ao qual o grupo de políticas pertence.

  Você especifica o SVM ao criar o grupo de políticas.

- Se você atribuir um LUN a um grupo de políticas, não será possível atribuir o volume ou SVM contendo LUN a um grupo de políticas.

Para obter mais informações sobre como usar QoS de armazenamento, consulte "Referência de administração do sistema".

Passos

1. Use o `qos policy-group create` comando para criar um grupo de políticas.
2. Use o `lun create` comando ou o `lun modify` comando com o `-qos-policy-group` parâmetro para atribuir um LUN a um grupo de políticas.
3. Use os `qos statistics` comandos para exibir dados de desempenho.
4. Se necessário, use o `qos policy-group modify` comando para ajustar o limite máximo de taxa de transferência do grupo de políticas.

Ferramentas disponíveis para monitorar seus LUNs de forma eficaz

Estão disponíveis ferramentas para o ajudar a monitorizar eficazmente os seus LUNs e evitar ficar sem espaço.

- O Active IQ Unified Manager é uma ferramenta gratuita que permite gerenciar todo o storage em todos os clusters do ambiente.
- O System Manager é uma interface gráfica de usuário incorporada ao ONTAP que permite gerenciar manualmente as necessidades de storage no nível do cluster.
- O OnCommand Insight apresenta uma visão única da sua infraestrutura de storage e permite configurar monitoramento automático, alertas e geração de relatórios quando LUNs, volumes e agregados estão ficando sem espaço de storage.

Funcionalidades e restrições de LUNs transicionados

Em um ambiente SAN, é necessária uma interrupção no serviço durante a transição de um volume de 7 modos para o ONTAP. Você precisa encerrar seus hosts para concluir a transição. Após a transição, você precisa atualizar as configurações de seu host antes de começar a fornecer dados no ONTAP

Você precisa agendar uma janela de manutenção durante a qual você pode encerrar seus hosts e concluir a transição.

Os LUNs transferidos do Data ONTAP que operam no modo 7 para o ONTAP têm certos recursos e restrições que afetam a maneira como os LUNs podem ser gerenciados.

Você pode fazer o seguinte com LUNs transicionados:

- Visualize o LUN usando o `lun show` comando
- Visualize o inventário de LUNs transferidos do volume do modo 7D usando o `transition 7-mode`

`show` comando

- Restaure um volume a partir de uma cópia Snapshot de 7 modos

  A restauração do volume faz a transição de todos os LUNs capturados na cópia Snapshot

- Restaure um único LUN a partir de uma cópia Snapshot de 7 modos usando o `snapshot restore-file` comando
- Crie um clone de um LUN em uma cópia Snapshot de 7 modos
- Restaure um intervalo de blocos a partir de um LUN capturado em uma cópia Snapshot de 7 modos
- Crie um FlexClone do volume usando uma cópia Snapshot do modo 7

Não é possível fazer o seguinte com LUNs transicionados:

- Acesse clones LUN com cópia Snapshot capturados no volume

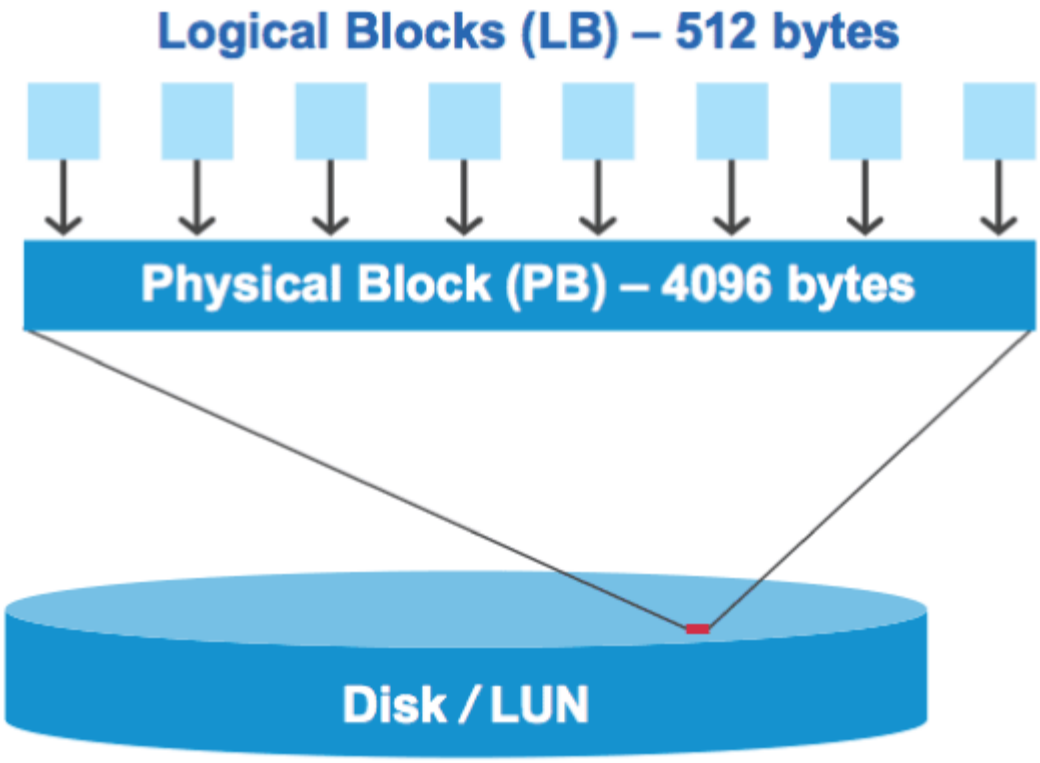
Informações relacionadas

"Transição baseada em cópia"

Desalinhamentos de e/S na visão geral dos LUNs alinhados adequadamente

O ONTAP pode relatar desalinhamentos de e/S em LUNs alinhados corretamente. Em geral, esses avisos de desalinhamento podem ser desconsiderados, desde que você esteja confiante de que seu LUN está corretamente provisionado e que sua tabela de particionamento está correta.

LUNs e discos rígidos fornecem armazenamento como blocos. Como o tamanho do bloco para discos no host é de 512 bytes, os LUNs apresentam blocos desse tamanho ao host, enquanto usam blocos maiores de 4 KB para armazenar dados. O bloco de dados de 512 bytes usado pelo host é referido como um bloco lógico. O bloco de dados de 4 KB usado pelo LUN para armazenar dados é referido como um bloco físico. Isso significa que existem oito blocos lógicos de 512 bytes em cada bloco físico de 4 KB.



O sistema operacional do host pode iniciar uma operação de e/S de leitura ou gravação em qualquer bloco lógico. As operações de e/S só são consideradas alinhadas quando começam no primeiro bloco lógico no bloco físico. Se uma operação de e/S começar em um bloco lógico que também não é o início de um bloco físico, a e/S é considerada desalinhada. O ONTAP deteta automaticamente o desalinhamento e informa-o no LUN. No entanto, a presença de e/S desalinhadas não significa necessariamente que o LUN também esteja desalinhado. É possível que e/S desalinhadas sejam relatadas em LUNs alinhados corretamente.

Se necessitar de mais investigação, consulte o artigo da base de dados de Conhecimento "Como identificar e/S desalinhadas em LUNs?"

Para obter mais informações sobre ferramentas para corrigir problemas de alinhamento, consulte a seguinte documentação

- "Utilitários do Windows Unified Host 7,1"
- "Provisione a documentação de storage SAN"

Obtenha alinhamento de e/S usando os tipos de SO LUN

Para o ONTAP 9.7 ou anterior, você deve usar o valor de LUN ONTAP `ostype` recomendado que mais corresponde ao seu sistema operacional para alcançar o alinhamento de e/S com o esquema de particionamento do sistema operacional.

O esquema de partição empregado pelo sistema operacional host é um fator importante que contribui para desalinhamentos de e/S. Alguns valores de LUN do ONTAP `ostype` usam um deslocamento especial conhecido como "prefixo" para permitir que o esquema de particionamento padrão usado pelo sistema operacional do host seja alinhado.

Em algumas circunstâncias, uma tabela de particionamento personalizada pode ser necessária para alcançar o alinhamento de e/S. No entanto, para `ostype` valores com um valor "'prefixo'" maior que `0`, uma partição personalizada pode criar e/S desalinhadas

Para obter mais informações sobre LUNs provisionados no ONTAP 9.7 ou anterior, consulte o artigo da KB "Como identificar e/S desalinhadas em LUNs".

Por padrão, os novos LUNs provisionados no ONTAP 9.8 ou posterior têm um tamanho de prefixo e sufixo de zero para todos os tipos de sistema operacional LUN. A e/S deve estar alinhada com o sistema operacional de host suportado por padrão.

Considerações especiais de alinhamento de e/S para Linux

As distribuições Linux oferecem uma ampla variedade de maneiras de usar um LUN, incluindo como dispositivos brutos para bancos de dados, vários gerenciadores de volume e sistemas de arquivos. Não é necessário criar partições em um LUN quando usado como um dispositivo bruto ou como volume físico em um volume lógico.

Para RHEL 5 e anteriores e SLES 10 e anteriores, se o LUN será usado sem um gerenciador de volume, você deve particionar o LUN para ter uma partição que começa em um deslocamento alinhado, que é um setor que é um mesmo múltiplo de oito blocos lógicos.

Considerações especiais de alinhamento de e/S para LUNs Solaris

Você precisa considerar vários fatores ao determinar se você deve usar o `solaris` ostype ou o ostype. `solaris_efi`

Consulte "Guia de instalação e administração dos Utilitários do Solaris Host" para obter informações detalhadas.

Os LUNs de inicialização do ESX relatam como desalinhados

Os LUNs usados como LUNs de inicialização do ESX geralmente são relatados pelo ONTAP como desalinhados. O ESX cria várias partições no LUN de inicialização, dificultando o alinhamento. LUNs de inicialização do ESX desalinhados geralmente não são um problema de desempenho porque a quantidade total de e/S desalinhados é pequena. Supondo que o LUN foi corretamente provisionado com o VMware `ostype`, nenhuma ação é necessária.

Informações relacionadas

"Alinhamento de partição/disco do sistema de arquivos VM convidada para VMware vSphere, outros ambientes virtuais e sistemas de storage NetApp"

Formas de resolver problemas quando os LUNs ficam offline

Quando não há espaço disponível para gravações, os LUNs ficam offline para preservar a integridade dos dados. Os LUNs podem ficar sem espaço e ficar offline por vários motivos, e há várias maneiras de resolver o problema.

Se o…	Você pode…
O agregado está cheio	• Adicione mais discos. • Use o `volume modify` comando para reduzir um volume que tenha espaço disponível. • Se você tiver volumes de garantia de espaço que tenham espaço disponível, altere a garantia de espaço de volume para `none` com o `volume modify` comando.
O volume está cheio, mas há espaço disponível no agregado contendo	• Para volumes de garantia de espaço, use o `volume modify` comando para aumentar o tamanho do seu volume. • Para volumes provisionados de forma fina, use o `volume modify` comando para aumentar o tamanho máximo do seu volume. Se o volume com crescimento automático não estiver ativado, `volume modify -autogrow -mode` utilize para o ativar. • Exclua cópias Snapshot manualmente com o `volume snapshot delete` comando ou use o `volume snapshot autodelete modify` comando para excluir cópias snapshot automaticamente.

Informações relacionadas

"Gerenciamento de disco e camada local (agregado)"

"Gerenciamento de storage lógico"

Solucionar problemas de LUNs iSCSI não visíveis no host

Os iSCSI LUNs aparecem como discos locais para o host. Se os LUNs do sistema de armazenamento não estiverem disponíveis como discos no host, você deverá verificar as configurações.

Definição de configuração	O que fazer
Cabeamento	Verifique se os cabos entre o host e o sistema de armazenamento estão conetados corretamente.

Definição de configuração	O que fazer
Conetividade de rede	Verifique se há conetividade TCP/IP entre o host e o sistema de armazenamento. • Na linha de comando do sistema de storage, faça ping nas interfaces de host que estão sendo usadas para iSCSI: `ping -node node_name -destination host_ip_address_for_iSCSI` • Na linha de comando do host, faça ping nas interfaces do sistema de storage que estão sendo usadas para iSCSI: `ping -node node_name -destination host_ip_address_for_iSCSI`
Requisitos do sistema	Verifique se os componentes da sua configuração estão qualificados. Além disso, verifique se você tem o nível correto de Service pack do sistema operacional do host (SO), a versão do iniciador, a versão do ONTAP e outros requisitos do sistema. A Matriz de interoperabilidade contém os requisitos de sistema mais atualizados.
Jumbo Frames	Se você estiver usando quadros jumbo em sua configuração, verifique se os quadros jumbo estão ativados em todos os dispositivos no caminho de rede: A NIC Ethernet do host, o sistema de armazenamento e quaisquer switches.
Estado do serviço iSCSI	Verifique se o serviço iSCSI está licenciado e iniciado no sistema de armazenamento.
Início de sessão do iniciador	Verifique se o iniciador está conetado ao sistema de armazenamento. Se o `iscsi initiator show` comando output não mostrar que nenhum iniciador está conetado, verifique a configuração do iniciador no host. Verifique também se o sistema de armazenamento está configurado como um destino do iniciador.
Nomes de nós iSCSI (IQNs)	Verifique se você está usando os nomes de nó do iniciador corretos na configuração do igroup. No host, você pode usar as ferramentas e os comandos do iniciador para exibir o nome do nó do iniciador. Os nomes de nós do iniciador configurados no grupo e no host devem corresponder.
Mapeamentos LUN	Verifique se os LUNs estão mapeados para um grupo. No console do sistema de storage, você pode usar um dos seguintes comandos: • `lun mapping show` Exibe todos os LUNs e os grupos para os quais são mapeados. • `lun mapping show -igroup` Exibe os LUNs mapeados para um grupo específico.
ISCSI LIFs habilitadas	Verifique se as interfaces lógicas iSCSI estão ativadas.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

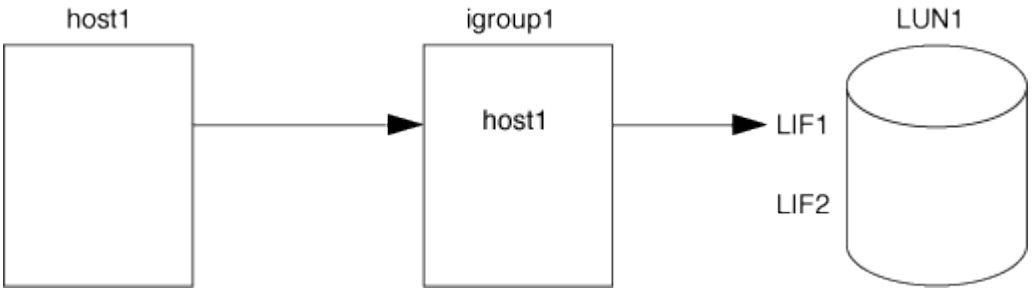
Gerencie grupos e portsets

Maneiras de limitar o acesso LUN com portsets e grupos

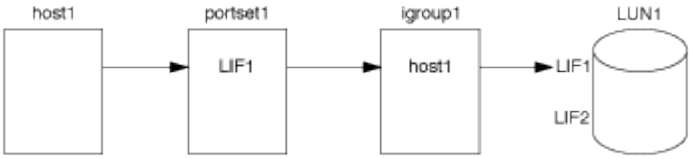
Além de usar o mapa LUN Seletivo (SLM), você pode limitar o acesso aos LUNs por meio de grupos e portsets.

Os Portsets podem ser usados com o SLM para restringir ainda mais o acesso de determinados alvos a certos iniciadores. Ao usar o SLM com portsets, os LUNs estarão acessíveis no conjunto de LIFs no portset no nó proprietário do LUN e no parceiro de HA desse nó.

No exemplo a seguir, initiator1 não tem um portset Sem um portset, initiator1 pode acessar LUN1 através de LIF1 e LIF2.



Você pode limitar o acesso ao LUN1 usando um portset No exemplo a seguir, o initiator1 pode acessar o LUN1 somente através do LIF1. No entanto, o initiator1 não pode acessar o LUN1 através do LIF2 porque o LIF2 não está no portset1.



Informações relacionadas

- Mapa LUN seletivo
- Criar um portset e ligar a um igroup

Visualizar e gerenciar iniciadores e grupos SAN

Você pode usar o System Manager para exibir e gerenciar grupos de iniciadores (grupos de iniciadores) e iniciadores.

Sobre esta tarefa

- Os grupos de iniciadores identificam quais hosts são capazes de acessar LUNs específicos no sistema de storage.
- Depois que um grupo de iniciadores e iniciadores forem criados, você também pode editá-los ou excluí-los.
- Para gerenciar grupos e iniciadores de SAN, você pode executar as seguintes tarefas:

- [view-manage-san-igroups]
- [view-manage-san-inits]

Exibir e gerenciar grupos de iniciadores SAN

Você pode usar o System Manager para exibir uma lista de grupos de iniciadores (grupos de iniciadores). Na lista, você pode executar operações adicionais.

Passos

1. No System Manager, clique em **hosts > SAN Initiator Groups**.

   A página exibe uma lista de grupos de iniciadores (grupos de iniciadores). Se a lista for grande, você pode visualizar páginas adicionais da lista clicando nos números de página no canto inferior direito da página.

   As colunas exibem várias informações sobre os grupos. A partir de 9.11.1, o estado da ligação do grupo também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

2. (Opcional): Você pode executar as seguintes tarefas clicando nos ícones no canto superior direito da lista:
   - **Pesquisa**
   - * Faça o download* da lista.
   - **Mostrar** ou **Ocultar** colunas na lista.
   - **Filtrar** os dados da lista.
3. Pode efetuar operações a partir da lista:
   - Clique + Add para adicionar um grupo.
   - Clique no nome do grupo para visualizar a página **Visão geral** que mostra detalhes sobre o grupo.

     Na página **Visão geral**, você pode exibir os LUNs associados ao grupo e iniciar as operações para criar LUNs e mapear os LUNs. Clique em **todos os iniciadores de SAN** para retornar à lista principal.
   - Passe o Mouse sobre o grupo e clique ⋮ ao lado de um nome do grupo para editar ou excluir o grupo.
   - Passe o Mouse sobre a área à esquerda do nome do grupo e marque a caixa de seleção. Se você clicar em * Adicionar ao Grupo Iniciador*, você pode adicionar esse grupo a outro grupo.
   - Na coluna **Storage VM**, clique no nome de uma VM de armazenamento para exibir detalhes sobre ela.

Exibir e gerenciar iniciadores de SAN

Você pode usar o System Manager para exibir uma lista de iniciadores. Na lista, você pode executar operações adicionais.

Passos

1. No System Manager, clique em **hosts > SAN Initiator Groups**.

   A página exibe uma lista de grupos de iniciadores (grupos de iniciadores).

2. Para visualizar os iniciadores, execute o seguinte:
   - Clique na guia **iniciadores FC** para exibir uma lista de iniciadores FC.
   - Clique no separador **iniciadores iSCSI** para ver uma lista de iniciadores iSCSI.

As colunas exibem várias informações sobre os iniciadores.

A partir de 9.11.1, o estado da ligação do iniciador também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

3. (Opcional): Você pode executar as seguintes tarefas clicando nos ícones no canto superior direito da lista:
   - **Pesquisar** a lista de iniciadores específicos.
   - * Faça o download* da lista.
   - **Mostrar** ou **Ocultar** colunas na lista.
   - **Filtrar** os dados da lista.

Crie um grupo aninhado

A partir do ONTAP 9.9,1, você pode criar um grupo que consiste em outros grupos existentes.

1. No System Manager, clique em **Host > SAN Initiator Groups** e, em seguida, clique em **Add**.
2. Digite o grupo **Nome** e **Descrição**.

   A descrição serve como o alias do igroup.

3. Selecione **Storage VM** e **Host Operating System**.

   O tipo de SO de um grupo aninhado não pode ser alterado depois que o grupo é criado.

4. Em **Membros do Grupo Iniciador** selecione **Grupo de iniciadores existente**.

   Você pode usar **Search** para localizar e selecionar os grupos de iniciadores que deseja adicionar.

Mapeie grupos para vários LUNs

A partir do ONTAP 9.9,1, é possível mapear grupos para dois ou mais LUNs simultaneamente.

1. No System Manager, clique em **Storage > LUNs**.
2. Selecione os LUNs que pretende mapear.
3. Clique em **mais** e, em seguida, clique em **Map to Initiator Groups**.

Os grupos selecionados são adicionados aos LUNs selecionados. Os mapeamentos pré-existentes não são sobrescritos.

Criar um portset e ligar a um igroup

Além de usar "Mapa LUN seletivo (SLM)"o , você pode criar um portset e vincular o portset a um grupo para limitar ainda mais os LIFs que podem ser usados por um iniciador para acessar um LUN.

Se você não vincular um portset a um grupo, todos os iniciadores do grupo podem acessar LUNs mapeados através de todas as LIFs no nó que possui o LUN e o parceiro HA do nó proprietário.

O que você vai precisar

Você deve ter pelo menos um LIF e um igrop.

A menos que você esteja usando grupos de interface, dois LIFs são recomendados para redundância para iSCSI e FC. Apenas um LIF é recomendado para grupos de interfaces.

Sobre esta tarefa

É vantajoso usar portsets com SLM quando você tem mais de duas LIFs em um nó e você deseja restringir um determinado iniciador a um subconjunto de LIFs. Sem portsets, todos os destinos no nó serão acessíveis por todos os iniciadores com acesso ao LUN por meio do nó proprietário do LUN e do parceiro de HA do nó proprietário.

Exemplo 16. Passos

System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para criar portsets e vinculá-los aos grupos.

Se você precisar criar um portset e vinculá-lo a um grupo em uma versão do ONTAP anterior a 9.10.1, você deve usar o procedimento da CLI do ONTAP.

1. No System Manager, clique em **Network > Overview > Portsets** e clique em **Add**.
2. Insira as informações para o novo portset e clique em **Add**.
3. Clique em **hosts > SAN Initiator Groups**.
4. Para ligar o portset a um novo grupo, clique em **Add**.

   Para vincular o portset a um grupo existente, selecione o grupo, clique em e, em seguida, clique em **Edit Initiator Group** (Editar grupo de iniciadores).

Informações relacionadas

"Visualizar e gerenciar iniciadores e grupos de trabalho"

CLI

1. Crie um conjunto de portas contendo os LIFs apropriados:

   `portset create -vserver` *`vserver_name`* `-portset` *`portset_name`* `-protocol` *`protocol`* `-port-name` *`port_name`*

   Se estiver usando FC, especifique o `protocol` parâmetro como `fcp`. Se estiver a utilizar iSCSI, especifique o `protocol` parâmetro como `iscsi`.

2. Vincule o grupo ao conjunto de portas:

   `lun igroup bind -vserver` *`vserver_name`* `-igroup` *`igroup_name`* `-portset` *`portset_name`*

3. Verifique se os conjuntos de portas e LIFs estão corretos:

   `portset show -vserver` *`vserver_name`*

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

Gerenciar portsets

Além "Mapa LUN seletivo (SLM)"do , você pode usar portsets para limitar ainda mais quais LIFs podem ser usados por um iniciador para acessar um LUN.

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para alterar as interfaces de rede

associadas a portsets e excluir portsets.

Altere as interfaces de rede associadas a um portset

1. No System Manager, selecione **rede > Visão geral > Portsets**.
2. Selecione o portset que pretende editar e, em seguida, selecione **Editar conjunto de portas**.

Eliminar um portset

1. No System Manager, clique em **rede > Visão geral > Portsets**.
2. Para eliminar um único portset, selecione o portset, selecione e, em seguida, selecione **Delete Portsets**.

   Para excluir vários portsets, selecione os portsets e clique em **Excluir**.

Descrição geral do mapa LUN seletivo

O mapa de LUN seletivo (SLM) reduz o número de caminhos do host para o LUN. Com o SLM, quando um novo mapa LUN é criado, o LUN só pode ser acessado por meio de caminhos no nó proprietário do LUN e de seu parceiro de HA.

O SLM permite o gerenciamento de um único grupo por host e também é compatível com operações de movimentação de LUN ininterruptas que não exigem manipulação de portset ou remapeamento de LUN.

"Portsets" Pode ser usado com o SLM para restringir ainda mais o acesso de determinados alvos a certos iniciadores. Ao usar o SLM com portsets, os LUNs estarão acessíveis no conjunto de LIFs no portset no nó proprietário do LUN e no parceiro de HA desse nó.

O SLM está ativado por predefinição em todos os novos mapas LUN.

Determine se o SLM está habilitado em um mapa LUN

Se o seu ambiente tiver uma combinação de LUNs criadas em uma versão do ONTAP 9 e LUNs transferidos de versões anteriores, talvez seja necessário determinar se o mapa de LUN seletivo (SLM) está habilitado em um LUN específico.

Você pode usar as informações exibidas na saída do `lun mapping show -fields reporting-nodes, node` comando para determinar se o SLM está habilitado no mapa LUN. Se o SLM não estiver habilitado, "-" será exibido nas células sob a coluna "'reportar nós'" da saída do comando. Se o SLM estiver ativado, a lista de nós exibida sob a coluna "'nós'" será duplicada na coluna "'reportar nós'".

Modifique a lista de nós de relatórios SLM

Se você estiver movendo um LUN ou um volume contendo LUNs para outro par de alta disponibilidade (HA) dentro do mesmo cluster, você deve modificar a lista de nós de relatórios de mapa de LUN seletivo (SLM) antes de iniciar a movimentação para garantir que os caminhos de LUN ativos e otimizados sejam mantidos.

Passos

1. Adicione o nó de destino e o nó de parceiro à lista de nós de relatório do agregado ou do volume:

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

Se você tiver uma convenção de nomenclatura consistente, poderá modificar vários mapeamentos de LUN ao mesmo tempo usando `igroup_prefix*` em vez `igroup_name` de .

2. Volte a digitalizar o host para descobrir os caminhos recém-adicionados.
3. Se o seu sistema operacional exigir isso, adicione os novos caminhos à configuração de e/S de rede multipath (MPIO).
4. Execute o comando para a operação de movimentação necessária e aguarde até que a operação termine.
5. Verifique se a e/S está sendo atendida pelo caminho Ativo/otimizado:

```
lun mapping show -fields reporting-nodes
```

6. Remova o proprietário do LUN anterior e o nó de parceiro da lista de nós de relatórios:

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. Verifique se o LUN foi removido do mapa LUN existente:

```
lun mapping show -fields reporting-nodes
```

8. Remova quaisquer entradas de dispositivo obsoletas para o sistema operacional do host.
9. Altere quaisquer arquivos de configuração de multipathing, se necessário.
10. Volte a digitalizar o host para verificar a remoção de caminhos antigos. Consulte a documentação do seu host para obter etapas específicas para verificar novamente seus hosts.

Gerir protocolo iSCSI

Configure a rede para obter o melhor desempenho

As redes Ethernet variam muito no desempenho. Pode maximizar o desempenho da rede utilizada para iSCSI selecionando valores de configuração específicos.

Passos

1. Conete o host e as portas de armazenamento à mesma rede.

   É melhor conetar-se aos mesmos interrutores. O roteamento nunca deve ser usado.

2. Selecione as portas de velocidade mais alta disponíveis e dedique-as ao iSCSI.

   As portas de 10 GbE são as melhores. As portas de 1 GbE são o mínimo.

3. Desative o controle de fluxo Ethernet para todas as portas.

   Você deve ver "Gerenciamento de rede" para usar a CLI para configurar o controle de fluxo da porta Ethernet.

4. Ative quadros jumbo (normalmente MTU de 9000).

   Todos os dispositivos no caminho de dados, incluindo iniciadores, destinos e switches, devem suportar quadros jumbo. Caso contrário, ativar quadros jumbo realmente reduz o desempenho da rede substancialmente.

Configurar um SVM para iSCSI

Para configurar uma máquina virtual de storage (SVM) para iSCSI, você deve criar LIFs para o SVM e atribuir o protocolo iSCSI a esses LIFs.

Sobre esta tarefa

Você precisa de, no mínimo, um iSCSI LIF por nó para cada SVM que forneça dados com o protocolo iSCSI. Para redundância, você deve criar pelo menos duas LIFs por nó.

Exemplo 17. Passos

System Manager

Configurar uma VM de armazenamento para iSCSI com o Gestor de sistema ONTAP (9,7 e posterior).

Para configurar iSCSI em uma nova VM de armazenamento	Para configurar iSCSI em uma VM de armazenamento existente
1. No System Manager, clique em **Storage > Storage VMs** e, em seguida, clique em **Add**. 2. Introduza um nome para a VM de armazenamento. 3. Selecione **iSCSI** para o **Protocolo de Acesso**. 4. Clique em **Enable iSCSI** (Ativar iSCSI) e introduza o endereço IP e a máscara de sub-rede para a interface de rede. Cada nó deve ter pelo menos duas interfaces de rede. 5. Clique em **Salvar**.	1. No System Manager, clique em **Storage > Storage VMs**. 2. Clique na VM de armazenamento que você deseja configurar. 3. Clique no separador **Definições** e, em seguida, clique em junto ao protocolo iSCSI. 4. Clique em **Enable iSCSI** (Ativar iSCSI) e introduza o endereço IP e a máscara de sub-rede para a interface de rede. Cada nó deve ter pelo menos duas interfaces de rede. 5. Clique em **Salvar**.

CLI

Configure uma VM de armazenamento para iSCSI com a CLI do ONTAP.

1. Ative os SVMs para ouvir tráfego iSCSI:

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. Crie um LIF para os SVMs em cada nó a ser usado para iSCSI:
   - Para o ONTAP 9.6 e posterior:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - Para o ONTAP 9.5 e versões anteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. Verifique se você configurou seus LIFs corretamente:

   ```
   network interface show -vserver vserver_name
   ```

4. Verifique se o iSCSI está ativo e em execução e o IQN de destino para esse SVM:

   ```
   vserver iscsi show –vserver vserver_name
   ```

5. A partir do seu host, crie sessões iSCSI para seus LIFs.

Informações relacionadas

"Relatório técnico da NetApp 4080: Práticas recomendadas para SAN moderna"

Defina um método de política de segurança para um iniciador

Você pode definir uma lista de iniciadores e seus métodos de autenticação. Você também pode modificar o método de autenticação padrão que se aplica a iniciadores que não possuem um método de autenticação definido pelo usuário.

Sobre esta tarefa

Você pode gerar senhas exclusivas usando algoritmos de política de segurança no produto ou especificar manualmente as senhas que deseja usar.

Nem todos os iniciadores suportam senhas secretas CHAP hexadecimais.

Passos

1. Use o `vserver iscsi security create` comando para criar um método de diretiva de segurança para um iniciador.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. Siga os comandos do ecrã para adicionar as palavras-passe.

   Cria um método de política de segurança para o iniciador iqn.1991-05.com.microsoft:host1 com nomes de usuário CHAP de entrada e saída e senhas.

Informações relacionadas

- Como a autenticação iSCSI funciona
- Autenticação CHAP

Excluir um serviço iSCSI de um SVM

Você pode excluir um serviço iSCSI de uma máquina virtual de armazenamento (SVM) se não for mais necessário.

O que você vai precisar

O status de administração do serviço iSCSI deve estar no estado "próprio" antes de poder excluir um serviço iSCSI. Você pode mover o status de administração para baixo com o `vserver iscsi modify` comando.

Passos

1. Use o `vserver iscsi modify` comando para parar a e/S para o LUN.

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. Use o `vserver iscsi delete` comando para remover o serviço iscsi do SVM.

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. Use o `vserver iscsi show command` para verificar se você excluiu o serviço iSCSI do SVM.

```
vserver iscsi show -vserver vs1
```

Obtenha mais detalhes em recuperações de erros de sessão iSCSI

Aumentar o nível de recuperação de erros de sessão iSCSI permite-lhe receber informações mais detalhadas sobre recuperações de erros iSCSI. O uso de um nível de recuperação de erros mais alto pode causar uma redução menor no desempenho da sessão iSCSI.

Sobre esta tarefa

Por padrão, o ONTAP é configurado para usar o nível de recuperação de erro 0 para sessões iSCSI. Se você estiver usando um iniciador que foi qualificado para o nível de recuperação de erros 1 ou 2, você pode optar por aumentar o nível de recuperação de erros. O nível de recuperação de erro de sessão modificado afeta apenas as sessões recém-criadas e não afeta as sessões existentes.

A partir do ONTAP 9.4, a `max-error-recovery-level` opção não é suportada `iscsi show` nos comandos e. `iscsi modify`

Passos

1. Entrar no modo avançado:

```
set -privilege advanced
```

2. Verifique a configuração atual usando o `iscsi show` comando.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
------- ------------------------
vs3     0
```

3. Altere o nível de recuperação de erros usando o `iscsi modify` comando.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

Registre o SVM em um servidor iSNS

Você pode usar o `vserver iscsi isns` comando para configurar a máquina virtual de armazenamento (SVM) para se Registrar em um servidor iSNS.

Sobre esta tarefa

O `vserver iscsi isns create` comando configura o SVM para se Registrar no servidor iSNS. O SVM não fornece comandos que permitem configurar ou gerenciar o servidor iSNS. Para gerenciar o servidor iSNS, você pode usar as ferramentas de administração do servidor ou a interface fornecida pelo fornecedor para o servidor iSNS.

Passos

1. No servidor iSNS, certifique-se de que o serviço iSNS está ativo e disponível para serviço.
2. Crie o LIF de gerenciamento de SVM em uma porta de dados:

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

3. Crie um serviço iSCSI no SVM se ainda não existir um:

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. Verifique se o serviço iSCSI foi criado com sucesso:

   ```
   iscsi show -vserver SVM_name
   ```

5. Verifique se existe uma rota padrão para o SVM:

   ```
   network route show -vserver SVM_name
   ```

6. Se uma rota padrão não existir para o SVM, crie uma rota padrão:

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

7. Configure o SVM para se Registrar no serviço iSNS:

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   As famílias de endereços IPv4 e IPv6 são apoiadas. A família de endereços do servidor iSNS deve ser a mesma do LIF de gerenciamento do SVM.

   Por exemplo, você não pode conetar um LIF de gerenciamento de SVM com um endereço IPv4 a um servidor iSNS com um endereço IPv6.

8. Verifique se o serviço iSNS está em execução:

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. Se o serviço iSNS não estiver em execução, inicie-o:

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

Resolva mensagens de erro iSCSI no sistema de armazenamento

Existem várias mensagens de erro comuns relacionadas ao iSCSI que podem ser visualizadas com o `event log show` comando. Você precisa saber o que essas mensagens significam e o que você pode fazer para resolver os problemas que elas identificam.

A tabela a seguir contém as mensagens de erro mais comuns e instruções para resolvê-las:

Mensagem	Explicação	O que fazer
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	O serviço iSCSI não está ativado na interface.	Pode utilizar o `iscsi interface enable` comando para ativar o serviço iSCSI na interface. Por exemplo: `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	O CHAP não está configurado corretamente para o iniciador especificado.	Deve verificar as definições CHAP; não pode utilizar o mesmo nome de utilizador e palavra-passe para as definições de entrada e saída no sistema de armazenamento: • As credenciais de entrada no sistema de storage devem corresponder às credenciais de saída no iniciador. • As credenciais de saída no sistema de storage devem corresponder às credenciais de entrada no iniciador.

Ativar ou desativar o failover automático de iSCSI LIF

Depois de atualizar para o ONTAP 9.11,1 ou posterior, deverá ativar manualmente o failover automático de LIF em todas as LIFs iSCSI criadas no ONTAP 9.10,1 ou anterior.

A partir do ONTAP 9.11,1, você pode ativar o failover automático de LIF para LIFs iSCSI em plataformas all-flash de storage SAN. Se ocorrer um failover de armazenamento, o iSCSI LIF é migrado automaticamente de seu nó ou porta inicial para o nó ou porta do parceiro de HA e, em seguida, volta assim que o failover for concluído. Ou, se a porta para iSCSI LIF não for saudável, o LIF é migrado automaticamente para uma porta saudável em seu nó inicial atual e, em seguida, de volta para sua porta original quando a porta estiver funcionando novamente. O permite que os workloads SAN executados no iSCSI retomem o serviço de e/S mais rapidamente após a ocorrência de um failover.

No ONTAP 9.11,1 e posterior, por padrão, os LIFs iSCSI recém-criados são ativados para failover automático de LIF se uma das seguintes condições for verdadeira:

- Não há iSCSI LIFs no SVM
- Todas as LIFs iSCSI na SVM são ativadas para failover automático de LIF

Ativar failover automático de LIF iSCSI

Por padrão, LIFs iSCSI criadas no ONTAP 9.10,1 e anteriores não são ativadas para failover automático de LIF. Se houver iSCSI LIFs na SVM que não estejam habilitadas para failover automático de LIF, seus LIFs recém-criados também não serão ativados para failover automático de LIF. Se o failover automático de LIF não estiver ativado e houver um evento de failover, seus iSCSI LIFs não serão migrados.

Saiba mais "Failover de LIF e giveback"sobre o .

Passo

1. Ativar failover automático para um iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

Para atualizar todas as LIFs iSCSI na SVM, use `-lif*` em vez `lif` de .

Desativar o failover automático de LIF iSCSI

Se você ativou anteriormente o failover automático de LIF iSCSI em LIFs iSCSI criados no ONTAP 9.10,1 ou anterior, você tem a opção de desativá-lo.

Passo

1. Desativar failover automático para um iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

Para atualizar todas as LIFs iSCSI na SVM, use `-lif*` em vez `lif` de .

Informações relacionadas

- "Crie um LIF"
- Manualmente "Migração de um LIF"
- Manualmente "Reverter um LIF para sua porta inicial"
- "Configure as configurações de failover em um LIF"

Gerenciar o protocolo FC

Configurar um SVM para FC

Para configurar uma máquina virtual de storage (SVM) para FC, você deve criar LIFs para o SVM e atribuir o protocolo FC a esses LIFs.

Antes de começar

Você deve ter uma licença FC ("Incluído no ONTAP One") e ela deve estar habilitada. Se a licença FC não estiver ativada, os LIFs e SVMs parecerão estar online, mas o status operacional será `down`. O serviço FC precisa estar habilitado para que seus LIFs e SVMs estejam operacionais. Você deve usar o zoneamento de iniciador único para todos os LIFs FC no SVM para hospedar os iniciadores.

Sobre esta tarefa

O NetApp dá suporte a pelo menos um FC LIF por nó para cada SVM, fornecendo dados com o protocolo FC. É necessário usar duas LIFs por nó e duas malhas, com um LIF por nó anexado. Isso fornece redundância na camada de nó e na malha.

Exemplo 18. Passos

System Manager

Configurar uma VM de armazenamento para iSCSI com o Gestor de sistema ONTAP (9,7 e posterior).

Para configurar o FC em uma nova VM de storage	Para configurar o FC em uma VM de storage existente
1. No System Manager, clique em **Storage > Storage VMs** e, em seguida, clique em **Add**. 2. Introduza um nome para a VM de armazenamento. 3. Selecione **FC** para o **Protocolo de Acesso**. 4. Clique em **Ativar FC**. As portas FC são atribuídas automaticamente. 5. Clique em **Salvar**.	1. No System Manager, clique em **Storage > Storage VMs**. 2. Clique na VM de armazenamento que você deseja configurar. 3. Clique na guia **Configurações** e, em seguida, clique ⚙ ao lado do protocolo FC. 4. Clique em **Enable FC** (Ativar FC) e introduza o endereço IP e a máscara de sub-rede para a interface de rede. As portas FC são atribuídas automaticamente. 5. Clique em **Salvar**.

CLI

1. Habilite o serviço FC na SVM:

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. Crie duas LIFs para as SVMs em cada nó que fornece FC:
   - Para o ONTAP 9.6 e posterior:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - Para o ONTAP 9.5 e versões anteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. Verifique se seus LIFs foram criados e se o status operacional deles é `online`:

   ```
   network interface show -vserver vserver_name lif_name
   ```

Informações relacionadas

"Suporte à NetApp"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Considerações para LIFs em ambientes SAN de cluster

Excluir um serviço FC de um SVM

Você pode excluir um serviço FC de uma máquina virtual de storage (SVM) se não for mais necessário.

O que você vai precisar

O status de administração deve ser "próprio" antes de excluir um serviço FC de um SVM. Você pode definir o status de administração para baixo com o `vserver fcp modify` comando ou o `vserver fcp stop` comando.

Passos

1. Use o `vserver fcp stop` comando para parar a e/S para o LUN.

   ```
   vserver fcp stop -vserver vs_1
   ```

2. Use o `vserver fcp delete` comando para remover o serviço da SVM.

   ```
   vserver fcp delete -vserver vs_1
   ```

3. Use o `vserver fcp show` para verificar se você excluiu o serviço FC do SVM:

   ```
   vserver fcp show -vserver vs_1
   ```

Configurações de MTU recomendadas para quadros jumbo FCoE

Para Fibre Channel over Ethernet (FCoE), os quadros jumbo para a parte do adaptador Ethernet da CNA devem ser configurados em 9000 MTU. Os frames grandes para a parte do adaptador FCoE da CNA devem ser configurados com mais de 1500 MTU. Apenas configure quadros jumbo se o iniciador, o alvo e todos os switches intervenientes suportarem e estiverem configurados para quadros jumbo.

Gerenciar o protocolo NVMe

Inicie o serviço NVMe em uma SVM

Antes de usar o protocolo NVMe na máquina virtual de storage (SVM), é necessário iniciar o serviço NVMe no SVM.

Antes de começar

O NVMe deve ser permitido como protocolo no seu sistema.

Os seguintes protocolos NVMe são compatíveis:

Protocolo	Começando com …	Permitido por…
TCP	ONTAP 9.10,1	Padrão
FCP	ONTAP 9,4	Padrão

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Verifique se o NVMe é permitido como protocolo:

   ```
   vserver nvme show
   ```

3. Criar o serviço de protocolo NVMe:

   ```
   vserver nvme create
   ```

4. Inicie o serviço de protocolo NVMe na SVM:

   ```
   vserver nvme modify -status -admin up
   ```

Excluir o serviço NVMe de um SVM

Se necessário, você pode excluir o serviço NVMe da sua máquina virtual de storage (SVM).

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Pare o serviço NVMe na SVM:

   ```
   vserver nvme modify -status -admin down
   ```

3. Exclua o serviço NVMe:

   ```
   vserver nvme delete
   ```

Redimensione um namespace

A partir do ONTAP 9.10,1, você pode usar a CLI do ONTAP para aumentar ou diminuir o tamanho de um namespace NVMe. Você pode usar o System Manager para aumentar o tamanho de um namespace NVMe.

Aumente o tamanho de um namespace

System Manager

1. Clique em **Storage > NVMe Namespaces**.
2. Passe o espaço de nomes que você deseja aumentar, clique em e, em seguida, clique em **Editar**.
3. Em **CAPACIDADE**, altere o tamanho do namespace.

CLI

1. Introduza o seguinte comando: `vserver nvme namespace modify -vserver SVM_name -path path –size new_size_of_namespace`

Diminua o tamanho de um namespace

Use a CLI do ONTAP para diminuir o tamanho de um namespace NVMe.

1. Altere a configuração de privilégios para avançado:

   ```
   set –privilege advanced
   ```

2. Diminua o tamanho do namespace:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
   ```

Converta um namespace em um LUN

A partir do ONTAP 9.11,1, você pode usar a CLI do ONTAP para converter no local um namespace NVMe existente em um LUN.

Antes de começar

- Namespace NVMe especificado não deve ter nenhum mapa existente para um subsistema.
- O namespace não deve fazer parte de uma cópia Snapshot ou no lado de destino da relação do SnapMirror como namespace somente leitura.
- Como os namespaces NVMe só são compatíveis com plataformas específicas e placas de rede, esse recurso funciona apenas com hardware específico.

Passos

1. Digite o seguinte comando para converter um namespace NVMe em um LUN:

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

Configurar a autenticação na banda pelo NVMe

A partir do ONTAP 9.12,1, você pode usar a interface de linha de comando (CLI) do ONTAP para configurar a autenticação na banda (segura), bidirecional e unidirecional entre um host e uma controladora NVMe através dos protocolos NVMe/TCP e NVMe/FC usando a autenticação DH-HMAC-CHAP. A partir do ONTAP 9.14,1, a autenticação na banda pode ser configurada no Gerenciador do sistema.

Para configurar a autenticação na banda, cada host ou controlador deve estar associado a uma chave DH-HMAC-CHAP, que é uma combinação do NQN do host ou controlador NVMe e um segredo de autenticação configurado pelo administrador. Para que um host ou controlador NVMe autentique seu peer, ele precisa saber a chave associada ao mesmo.

Na autenticação unidirecional, uma chave secreta é configurada para o host, mas não para o controlador. Na autenticação bidirecional, uma chave secreta é configurada para o host e para o controlador.

Sha-256 é a função hash padrão e 2048-bit é o grupo DH padrão.

System Manager

A partir do ONTAP 9.14,1, é possível usar o Gerenciador do sistema para configurar a autenticação na banda ao criar ou atualizar um subsistema NVMe, criar ou clonar espaços de nomes NVMe ou adicionar grupos de consistência com novos namespaces NVMe.

Passos

1. No System Manager, clique em **hosts > NVMe Subsystem** e, em seguida, clique em **Add**.
2. Adicione o nome do subsistema NVMe e selecione a VM de storage e o sistema operacional de host.
3. Introduza o NQN do anfitrião.
4. Selecione **Use in-band Authentication** ao lado do Host NQN.
5. Forneça o segredo do host e o segredo do controlador.

   A chave DH-HMAC-CHAP é uma combinação do NQN do host ou controlador NVMe e um segredo de autenticação configurado pelo administrador.

6. Selecione a função hash preferida e o grupo DH para cada host.

   Se você não selecionar uma função hash e um grupo DH, SHA-256 é atribuído como a função hash padrão e 2048 bits é atribuído como o grupo DH padrão.

7. Opcionalmente, clique em **Add** e repita as etapas conforme necessário para adicionar mais host.
8. Clique em **Salvar**.
9. Para verificar se a autenticação na banda está ativada, clique em **System Manager > hosts > NVMe Subsystem > Grid > Peek view**.

   Um ícone de chave transparente ao lado do nome do host indica que o modo unidirecional está ativado. Uma tecla opaca ao lado do nome do host indica que o modo bidirecional está ativado.

CLI

Passos

1. Adicione a autenticação DH-HMAC-CHAP ao subsistema NVMe:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

2. Verifique se o protocolo de autenticação DH-HMAC CHAP foi adicionado ao seu host:

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

3. Verifique se a autenticação DH-HMAC CHAP foi executada durante a criação do controlador NVMe:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Desativar a autenticação na banda pelo NVMe

Se você configurou a autenticação na banda pelo NVMe usando DH-HMAC-CHAP, você pode optar por desativá-la a qualquer momento.

Se estiver a reverter do ONTAP 9.12,1 ou posterior para o ONTAP 9.12,0 ou anterior, tem de desativar a autenticação na banda antes de reverter. Se a autenticação na banda usando DH-HMAC-CHAP não estiver desativada, a reversão falhará.

Passos

1. Remova o host do subsistema para desativar a autenticação DH-HMAC-CHAP:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verifique se o protocolo de autenticação DH-HMAC-CHAP foi removido do host:

```
vserver nvme subsystem host show
```

3. Adicione o host de volta ao subsistema sem autenticação:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Configurar o canal seguro TLS para NVMe/TCP

A partir do ONTAP 9.16,1, você pode configurar o canal seguro TLS para conexões NVMe/TCP. Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para adicionar um novo subsistema NVMe com TLS habilitado ou habilitar o TLS para um subsistema NVMe existente.

System Manager

A partir do ONTAP 9.16,1, você pode usar o Gerenciador de sistemas para configurar o TLS para conexões NVMe/TCP ao criar ou atualizar um subsistema NVMe, criar ou clonar espaços de nomes NVMe ou adicionar grupos de consistência com novos namespaces NVMe.

Passos

1. No System Manager, clique em **hosts > NVMe Subsystem** e, em seguida, clique em **Add**.
2. Adicione o nome do subsistema NVMe e selecione a VM de storage e o sistema operacional de host.
3. Introduza o NQN do anfitrião.
4. Selecione **Require Transport Layer Security (TLS)** ao lado do NQN do host.
5. Forneça a chave pré-compartilhada (PSK).
6. Clique em **Salvar**.
7. Para verificar se o canal seguro TLS está ativado, selecione **System Manager > hosts > NVMe Subsystem > Grid > Peek view**.

CLI

Passos

1. Adicione um host de subsistema NVMe compatível com o canal seguro TLS. Você pode fornecer uma chave pré-compartilhada (PSK) usando o `tls-configured-psk` argumento, ou usar um PSK gerado usando o `tls-generated-psk` argumento:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> {-tls-configured-psk <key_text> |
-tls-generated-psk true}
```

2. Verifique se o host do subsistema NVMe está configurado para o canal seguro TLS. Opcionalmente, você pode usar o `tls-key-type` argumento para exibir somente os hosts que estão usando esse tipo de chave:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured|generated}
```

3. Verifique se a controladora de host do subsistema NVMe está configurada para o canal seguro TLS. Opcionalmente, você pode usar qualquer um dos `tls-key-type` argumentos , `tls-identity` ou `tls-cipher` para exibir somente os controladores que têm esses atributos TLS:

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured|generated} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "adicionar o host do subsistema nvme do svm"
- "mostra o host do subsistema nvme do svm"
- "o controlador do subsistema do svm nvme mostra"

Desative o canal seguro TLS para NVMe/TCP

A partir do ONTAP 9.16,1, você pode configurar o canal seguro TLS para conexões NVMe/TCP. Se você configurou o canal seguro TLS para conexões NVMe/TCP, pode optar por desativá-lo a qualquer momento.

Passos

1. Remova o host do subsistema para desativar o canal seguro TLS:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verifique se o canal seguro TLS é removido do host:

```
vserver nvme subsystem host show
```

3. Adicione o host de volta ao subsistema sem o canal seguro TLS:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "adicionar o host do subsistema nvme do svm"
- "remoção do host do subsistema nvme do svm"
- "mostra o host do subsistema nvme do svm"

Alterar a prioridade do host NVMe

A partir do ONTAP 9.14,1, você pode configurar o subsistema NVMe para priorizar a alocação de recursos para hosts específicos. Por padrão, quando um host é adicionado ao subsistema, é atribuída uma prioridade regular. Os hosts atribuídos a uma alta prioridade são alocadas contagens de filas de e/S maiores e profundidades de filas.

Você pode usar a interface de linha de comando (CLI) do ONTAP para alterar manualmente a prioridade padrão de regular para alta. Para alterar a prioridade atribuída a um host, você deve remover o host do

subsistema e adicioná-lo de volta.

Passos

1. Verifique se a prioridade do host está definida como regular:

```
vserver nvme show-host-priority
```

2. Remova o host do subsistema:

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

3. Verifique se o host foi removido do subsistema:

```
vserver nvme subsystem host show
```

4. Adicione o host de volta ao subsistema com alta prioridade:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Gerenciar a detecção automatizada de host das controladoras NVMe/TCP

A partir do ONTAP 9.14,1, a descoberta de hosts de controladoras usando o protocolo NVMe/TCP é automatizada por padrão em malhas baseadas em IP.

Habilitar a detecção automatizada de host das controladoras NVMe/TCP

Se você desativou anteriormente a descoberta automatizada de host, mas suas necessidades foram alteradas, você pode reativá-la.

Passos

1. Entrar no modo de privilégio avançado:

```
set -privilege advanced
```

2. Ativar a deteção automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Verifique se a detecção automatizada de controladores NVMe/TCP está ativada.

```
vserver nvme show
```

Desativar a descoberta automatizada de host das controladoras NVMe/TCP

Se você não precisar que controladores NVMe/TCP sejam detetados automaticamente pelo host e detetar tráfego multicast indesejado na rede, desative essa funcionalidade.

Passos

1. Entrar no modo de privilégio avançado:

```
set -privilege advanced
```

2. Desativar a deteção automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Verifique se a detecção automatizada de controladores NVMe/TCP está desativada.

```
vserver nvme show
```

Desative o identificador da máquina virtual do host NVMe

A partir do ONTAP 9.14,1, por padrão, o ONTAP oferece suporte à capacidade de hosts NVMe/FC identificarem máquinas virtuais por um identificador exclusivo e de hosts NVMe/FC monitorarem a utilização de recursos da máquina virtual. Isso aprimora a geração de relatórios e a solução de problemas no lado do host.

Você pode usar o bootarg para desativar essa funcionalidade.

Passo

1. Desative o identificador da máquina virtual:

```
bootargs set fct_sli_appid_off <port>, <port>
```

O exemplo a seguir desativa o VMID na porta 0g e na porta 0i.

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

Gerenciar sistemas com adaptadores FC

Gerenciar sistemas com adaptadores FC

Os comandos estão disponíveis para gerenciar adaptadores FC integrados e placas adaptadoras FC. Esses comandos podem ser usados para configurar o modo do adaptador, exibir informações do adaptador e alterar a velocidade.

A maioria dos sistemas de storage tem adaptadores FC integrados que podem ser configurados como iniciadores ou destinos. Você também pode usar placas de adaptador FC configuradas como iniciadores ou destinos. Os iniciadores se conetam aos compartimentos de disco back-end e, possivelmente, a matrizes de armazenamento estranho (FlexArray). Os destinos se conetam apenas aos switches FC. Ambas as portas HBA de destino FC e a velocidade da porta do switch devem ser definidas para o mesmo valor e não devem ser definidas para auto.

Informações relacionadas

"Configuração SAN"

Comandos para gerenciar adaptadores FC

Você pode usar comandos FC para gerenciar adaptadores de destino FC, adaptadores iniciadores FC e adaptadores FC integrados para o controlador de storage. Os mesmos comandos são usados para gerenciar adaptadores FC para o protocolo FC e o protocolo FC-NVMe.

Os comandos do adaptador do iniciador FC funcionam apenas no nível do nó. Você deve usar o `run -node node_name` comando antes de usar os comandos do adaptador do iniciador FC.

Comandos para gerenciar adaptadores de destino FC

Se você quiser…	Use este comando…
Exibir as informações do adaptador FC em um nó	`network fcp adapter show`
Modifique os parâmetros do adaptador de destino FC	`network fcp adapter modify`
Apresentar informações de tráfego do protocolo FC	`run -node node_name sysstat -f`
Apresentar durante quanto tempo o protocolo FC foi executado	`run -node node_name uptime`

Se você quiser…	Use este comando…
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`
Exibir uma página de manual para um comando	`man command_name`

Comandos para gerenciar adaptadores de iniciador FC

Se você quiser…	Use este comando…
Exibir informações para todos os iniciadores e seus adaptadores em um nó	`run -node node_name storage show adapter`
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`

Comandos para gerenciar adaptadores FC integrados

Se você quiser…	Use este comando…
Exibir o status das portas FC integradas	`run -node node_name system hardware unified-connect show`

Configurar adaptadores FC

Cada porta FC integrada pode ser configurada individualmente como iniciador ou destino. As portas em certos adaptadores FC também podem ser configuradas individualmente como uma porta de destino ou uma porta de iniciador, assim como as portas FC integradas. Uma lista de adaptadores que podem ser configurados para o modo de destino está disponível no "NetApp Hardware Universe".

O modo de destino é usado para conetar as portas aos iniciadores FC. O modo iniciador é usado para conetar as portas a unidades de fita, bibliotecas de fita ou armazenamento de terceiros com virtualização FlexArray ou importação de LUN estrangeiro (FLI).

As mesmas etapas são usadas na configuração de adaptadores FC para o protocolo FC e para o protocolo FC-NVMe. No entanto, apenas certos adaptadores FC são compatíveis com FC-NVMe. Consulte "NetApp Hardware Universe" a para obter uma lista de adaptadores compatíveis com o protocolo FC-NVMe.

Configurar adaptadores FC para o modo de destino

Passos

1. Coloque o adaptador offline:

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

2. Altere o adaptador do iniciador para o destino:

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. Reinicie o nó que hospeda o adaptador que você alterou.
4. Verifique se a porta de destino tem a configuração correta:

   ```
   network fcp adapter show -node node_name
   ```

5. Coloque o adaptador online:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

Configurar adaptadores FC para o modo iniciador

O que você vai precisar

- Os LIFs no adaptador devem ser removidos de quaisquer conjuntos de portas dos quais sejam membros.
- Todos os LIF de todas as máquinas virtuais de armazenamento (SVM) que usam a porta física a ser modificada devem ser migrados ou destruídos antes de alterar a personalidade da porta física de destino para iniciador.

O NVMe/FC oferece suporte ao modo iniciador.

Passos

1. Remova todas as LIFs do adaptador:

   ```
   network interface delete -vserver SVM_name -lif LIF_name,LIF_name
   ```

2. Coloque o adaptador offline:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -status-admin
   down
   ```

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

3. Altere o adaptador de destino para iniciador:

   ```
   system hardware unified-connect modify -t initiator adapter_port
   ```

4. Reinicie o nó que hospeda o adaptador que você alterou.

5. Verifique se as portas FC estão configuradas no estado correto para sua configuração:

   `system hardware unified-connect show`

6. Coloque o adaptador novamente online:

   `node run -node node_name storage enable adapter adapter_port`

Ver as definições do adaptador

Você pode usar comandos específicos para exibir informações sobre seus adaptadores FC/UTA.

Adaptador de destino FC

Passo

1. Use o `network fcp adapter show` comando para exibir informações do adaptador: `network fcp adapter show -instance -node node1 -adapter 0a`

   A saída exibe informações de configuração do sistema e informações do adaptador para cada slot usado.

Adaptador de destino unificado (UTA) X1143A-R6

Passos

1. Inicialize seu controlador sem os cabos conetados.
2. Execute o `system hardware unified-connect show` comando para ver a configuração da porta e os módulos.
3. Visualize as informações da porta antes de configurar o CNA e as portas.

Altere a porta UTA2 do modo CNA para o modo FC

Você deve alterar a porta UTA2 do modo de adaptador de rede convergente (CNA) para o modo Fibre Channel (FC) para suportar o iniciador FC e o modo de destino FC. Você deve alterar a personalidade do modo CNA para o modo FC quando precisar alterar o meio físico que coneta a porta à sua rede.

Passos

1. Coloque o adaptador offline:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

2. Alterar o modo de porta:

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. Reinicie o nó e, em seguida, coloque o adaptador online:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

4. Notifique seu administrador ou gerenciador de VIF para excluir ou remover a porta, conforme aplicável:

   - Se a porta for usada como uma porta inicial de um LIF, for um membro de um grupo de interfaces (ifgrp) ou hosts VLANs, então um administrador deve fazer o seguinte:
     i. Mova os LIFs, remova a porta do ifgrp ou exclua as VLANs, respetivamente.
     ii. Exclua manualmente a porta executando o `network port delete` comando.

     Se o `network port delete` comando falhar, o administrador deve resolver os erros e, em seguida, executar o comando novamente.

   - Se a porta não for usada como porta inicial de um LIF, não for membro de um ifgrp e não hospedar VLANs, o gerenciador de VIF deve remover a porta de seus Registros no momento da reinicialização.

     Se o gerenciador de VIF não remover a porta, o administrador deve removê-la manualmente após a reinicialização usando o `network port delete` comando.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                      Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10     -
    e0f       Default      Default          down 1500  auto/10     -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0
```

```
    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. Verifique se você tem o SFP correto instalado:

   `network fcp adapter show -instance -node -adapter`

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB antes de alterar a configuração no nó.

Altere os módulos óticos do adaptador de destino CNA/UTA2

Você deve alterar os módulos óticos no adaptador de destino unificado (CNA/UTA2) para suportar o modo de personalidade que você selecionou para o adaptador.

Passos

1. Verifique o SFP atual usado na placa. Em seguida, substitua o SFP atual pelo SFP apropriado para a personalidade preferida (FC ou CNA).
2. Remova os módulos óticos atuais do adaptador X1143A-R6.

3. Insira os módulos corretos para a ótica do seu modo de personalidade (FC ou CNA) preferido.
4. Verifique se você tem o SFP correto instalado:

   `network fcp adapter show -instance -node -adapter`

   Módulos SFP suportados e cabos de cobre (Twinax) da marca Cisco estão listados no *Hardware Universe*.

Informações relacionadas

"NetApp Hardware Universe"

Configurações de porta suportadas para adaptadores X1143A-R6

O modo de destino FC é a configuração padrão para portas de adaptador X1143A-R6. No entanto, as portas desse adaptador podem ser configuradas como portas Ethernet e FCoE de 10 GB ou como portas FC de 16 GB.

Quando configurados para Ethernet e FCoE, os adaptadores X1143A-R6 suportam NIC concorrente e tráfego de destino FCoE na mesma porta de 10 GBE. Quando configurado para FC, cada par de duas portas que compartilha o mesmo ASIC pode ser configurado individualmente para o modo de iniciador FC ou destino. Isso significa que um único adaptador X1143A-R6 pode oferecer suporte ao modo de destino FC em um par de duas portas e no modo iniciador FC em outro par de duas portas.

Informações relacionadas

"NetApp Hardware Universe"

"Configuração SAN"

Configure as portas

Para configurar o adaptador de destino unificado (X1143A-R6), você deve configurar as duas portas adjacentes no mesmo chip no mesmo modo de personalidade.

Passos

1. Configure as portas conforme necessário para Fibre Channel (FC) ou adaptador de rede convergente (CNA) usando o `system node hardware unified-connect modify` comando.
2. Conete os cabos apropriados para FC ou Ethernet de 10 GB.
3. Verifique se você tem o SFP correto instalado:

   `network fcp adapter show -instance -node -adapter`

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB, com base na malha FC conetada.

Evite a perda de conetividade ao usar o adaptador X1133A-R6

Você pode evitar a perda de conetividade durante uma falha de porta configurando o sistema com caminhos redundantes para separar HBAs X1133A-R6.

O HBA X1133A-R6 é um adaptador FC de 4 portas e 16 GB que consiste em dois pares de 2 portas. O adaptador X1133A-R6 pode ser configurado como modo de destino ou modo de iniciador. Cada par de 2

portas é suportado por um único ASIC (por exemplo, porta 1 e porta 2 no ASIC 1 e porta 3 e porta 4 no ASIC 2). Ambas as portas em um único ASIC devem ser configuradas para operar no mesmo modo, seja no modo de destino ou no modo de iniciador. Se ocorrer um erro com o ASIC que suporta um par, ambas as portas do par ficam offline.

Para evitar essa perda de conetividade, configure o sistema com caminhos redundantes para separar HBAs X1133A-R6 ou com caminhos redundantes para portas compatíveis com ASICs diferentes no HBA.

Gerenciar LIFs para todos os protocolos SAN

Gerenciar LIFs para todos os protocolos SAN

Os iniciadores devem usar o Multipath I/o (MPIO) e o Asymmetric Logical Unit Access (ALUA) para capacidade de failover para clusters em um ambiente SAN. Se um nó falhar, os LIFs não migram nem assumem os endereços IP do nó do parceiro com falha. Em vez disso, o software MPIO, usando ALUA no host, é responsável por selecionar os caminhos apropriados para o acesso LUN por meio de LIFs.

É necessário criar um ou mais caminhos iSCSI a partir de cada nó em um par de HA, usando interfaces lógicas (LIFs) para permitir acesso a LUNs atendidas pelo par de HA. Você deve configurar um LIF de gerenciamento para cada máquina virtual de storage (SVM) que suporte SAN.

A conexão direta ou o uso de switches Ethernet são suportados para conetividade. Você deve criar LIFs para ambos os tipos de conetividade.

- Você deve configurar um LIF de gerenciamento para cada máquina virtual de storage (SVM) que suporte SAN. Você pode configurar duas LIFs por nó, uma para cada malha que está sendo usada com FC e para separar redes Ethernet para iSCSI.

Após a criação dos LIFs, eles podem ser removidos de conjuntos de portas, movidos para nós diferentes dentro de uma máquina virtual de storage (SVM) e excluídos.

Informações relacionadas

- "Configure a visão geral dos LIFs"
- "Crie um LIF"

Configurar um NVMe LIF

Certos requisitos devem ser atendidos ao configurar as LIFs do NVMe.

Antes de começar

O NVMe precisa ser compatível com o adaptador FC no qual você cria o LIF. Os adaptadores suportados estão listados em "Hardware Universe".

Sobre esta tarefa

A partir do ONTAP 9.12,1 e posterior, é possível configurar duas LIFs NVMe por nó em um máximo de 12 nós. No ONTAP 9.11,1 e versões anteriores, é possível configurar duas LIFs NVMe por nó no máximo dois nós.

As regras a seguir se aplicam ao criar um LIF NVMe:

- O NVMe pode ser o único protocolo de dados em LIFs de dados.

- Você deve configurar um LIF de gerenciamento para cada SVM compatível com SAN.
- Para o ONTAP 9.5 e posterior, você precisa configurar um LIF NVMe no nó que contém o namespace e o parceiro de HA do nó.
- Apenas para o ONTAP 9.4:
  - Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
  - Somente um LIF de dados NVMe pode ser configurado por SVM.

Passos

1. Crie o LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

NVMe/TCP está disponível a partir do ONTAP 9.10,1 e posterior.

2. Verifique se o LIF foi criado:

```
network interface show -vserver <SVM_name>
```

Após a criação, os LIFs NVMe/TCP escutam a descoberta na porta 8009.

O que saber antes de mover um SAN LIF

Você só precisa executar um movimento de LIF se estiver alterando o conteúdo do cluster, por exemplo, adicionando nós ao cluster ou excluindo nós do cluster. Se você executar um movimento de LIF, não será necessário rezonear sua malha FC ou criar novas sessões iSCSI entre os hosts anexados do cluster e a nova interface de destino.

Você não pode mover um SAN LIF usando o `network interface move` comando. O movimento DE SAN LIF deve ser realizado colocando o LIF offline, movendo o LIF para um nó ou porta inicial diferente e, em seguida, trazendo-o de volta on-line em sua nova localização. O Acesso lógico-Unidade assimétrica (ALUA) fornece caminhos redundantes e seleção automática de caminhos como parte de qualquer solução de SAN ONTAP. Portanto, não há interrupção de e/S quando o LIF é colocado off-line para o movimento. O host simplesmente tenta novamente e depois move I/o para outro LIF.

Ao usar o movimento LIF, você pode fazer o seguinte sem interrupções:

- Substitua um par de HA de um cluster por um par de HA atualizado de uma forma transparente para os hosts que acessam dados LUN
- Atualize uma placa de interface de destino
- Mova os recursos de uma máquina virtual de storage (SVM) de um conjunto de nós em um cluster para outro conjunto de nós no cluster

Remova um SAN LIF de um conjunto de portas

Se o LIF que você deseja excluir ou mover estiver em um conjunto de portas, você deve remover o LIF do conjunto de portas antes de excluir ou mover o LIF.

Sobre esta tarefa

Você precisa executar o passo 1 no procedimento a seguir somente se um LIF estiver no conjunto de portas. Não é possível remover o último LIF em um conjunto de portas se o conjunto de portas estiver vinculado a um grupo de iniciadores. Caso contrário, você pode começar com a Etapa 2 se várias LIFs estiverem no conjunto de portas.

Passos

1. Se apenas um LIF estiver no conjunto de portas, use o `lun igroup unbind` comando para desvincular o conjunto de portas do grupo de iniciadores.

   > Quando você desvincula um grupo de iniciadores de um conjunto de portas, todos os iniciadores do grupo de iniciadores têm acesso a todos os LUNs de destino mapeados para o grupo de iniciadores em todas as interfaces de rede.

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

2. Use o `lun portset remove` comando para remover o LIF do conjunto de portas.

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

Mova um SAN LIF

Se um nó precisar ficar offline, você pode mover um SAN LIF para preservar suas informações de configuração, como o WWPN, e evitar o zoneamento da malha do switch. Como um LIF SAN deve ser colocado off-line antes de ser movido, o tráfego de host deve confiar no software de multipathing de host para fornecer acesso sem interrupções ao LUN. É possível mover SAN LIFs para qualquer nó em um cluster, mas não é possível mover os SAN LIFs entre máquinas virtuais de armazenamento (SVMs).

O que você vai precisar

Se o LIF for um membro de um conjunto de portas, o LIF deve ter sido removido do conjunto de portas antes que o LIF possa ser movido para um nó diferente.

Sobre esta tarefa

O nó de destino e a porta física de um LIF que você deseja mover devem estar na mesma malha FC ou rede Ethernet. Se você mover um LIF para uma malha diferente que não tenha sido corretamente zoneada ou se você mover um LIF para uma rede Ethernet que não tenha conetividade entre o iniciador iSCSI e o destino, o LUN ficará inacessível quando você o colocar novamente on-line.

Passos

1. Veja o status administrativo e operacional do LIF:

   ```
   network interface show -vserver vserver_name
   ```

2. Altere o status do LIF para `down` (offline):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin
down
```

3. Atribua ao LIF um novo nó e porta:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node_name -home-port port_name
```

4. Altere o status do LIF para `up` (online):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

5. Verifique as alterações:

```
network interface show -vserver vserver_name
```

Exclua um LIF em um ambiente SAN

Antes de excluir um LIF, você deve garantir que o host conetado ao LIF possa acessar as LUNs por outro caminho.

O que você vai precisar

Se o LIF que você deseja excluir for membro de um conjunto de portas, primeiro remova o LIF do conjunto de portas antes de excluir o LIF.

System Manager

Exclua um LIF com o Gerenciador do sistema ONTAP (9,7 e posterior).

Passos

1. No System Manager, clique em **rede > Visão geral** e selecione **interfaces de rede**.
2. Selecione a VM de armazenamento a partir da qual você deseja excluir o LIF.
3. Clique ⋮ e selecione **Excluir**.

CLI

Exclua um LIF com a CLI do ONTAP.

Passos

1. Verifique o nome do LIF e da porta atual a serem excluídos:

   ```
   network interface show –vserver vserver_name
   ```

2. Eliminar o LIF:

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

3. Verifique se você excluiu o LIF:

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                    Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

Requisitos de SAN LIF para adicionar nós a um cluster

Você precisa estar ciente de certas considerações ao adicionar nós a um cluster.

- É necessário criar LIFs nos novos nós conforme apropriado antes de criar LUNs nesses novos nós.
- É necessário descobrir esses LIFs dos hosts conforme ditado pela pilha e pelo protocolo de host.

- Você deve criar LIFs nos novos nós para que os movimentos de LUN e volume sejam possíveis sem usar a rede de interconexão de cluster.

Configure iSCSI LIFs para retornar FQDN para hospedar a operação iSCSI SendTargets Discovery

A partir do ONTAP 9, os LIFs iSCSI podem ser configurados para retornar um nome de domínio totalmente qualificado (FQDN) quando um sistema operacional host envia uma operação de descoberta de SendTargets iSCSI. Retornar um FQDN é útil quando há um dispositivo NAT (Network Address Translation) entre o sistema operacional do host e o serviço de armazenamento.

Sobre esta tarefa

Os endereços IP de um lado do dispositivo NAT não têm sentido no outro lado, mas os FQDNs podem ter significado em ambos os lados.

> O limite de interoperabilidade do valor FQDN é de 128 carateres em todos os sistemas operacionais host.

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Configurar iSCSI LIFs para retornar FQDN:

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   No exemplo a seguir, os LIFs iSCSI são configurados para retornar storagehost-005.example.com como FQDN.

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. Verifique se sendtargets é o FQDN:

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   Neste exemplo, storagehost-005.example.com é exibido no campo de saída sendtargets-fqdn.

   ```
   cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
   sendtargets-fqdn
   vserver lif        sendtargets-fqdn
   ------- ---------- --------------------------
   vs1     vs1_iscsi1 storagehost-005.example.com
   vs1     vs1_iscsi2 storagehost-006.example.com
   ```

Informações relacionadas

"Referência do comando ONTAP"

Ativar a alocação de espaço ONTAP para protocolos SAN

A alocação de espaço do ONTAP ajuda a impedir que seus LUNs ou namespaces NVMe fiquem offline se eles ficarem sem espaço e permitir que seus hosts SAN recuperem espaço.

O suporte da ONTAP para alocação de espaço é baseado no protocolo SAN e na versão do ONTAP. A partir do ONTAP 9.16,1, a alocação de espaço é habilitada por padrão para protocolos iSCSI, FC e NVMe para todos os LUNs e namespaces recém-criados.

Versão de ONTAP	Protocolos	A alocação de espaço é…
9.16.1 ou posterior	• ISCSI • FC • NVMe	Habilitado por padrão para LUNs e namespaces recém-criados
9.15.1	• ISCSI • FC	Habilitado por padrão para LUNs recém-criados
	NVMe	Não suportado
9.14.1 e anteriores	• ISCSI • FC	Desativado por padrão para LUNs recém-criados
	NVMe	Não suportado

Quando a alocação de espaço está ativada:

- Se um LUN ou namespace ficar sem espaço, o ONTAP se comunica com o host que nenhum espaço livre está disponível para operações de gravação. Como resultado, o LUN ou namespace permanece on-line e as operações de leitura continuam sendo atendidas. Dependendo da configuração do host, o host tenta novamente as operações de gravação até que ele seja bem-sucedido ou o sistema de arquivos do host seja colocado offline. As operações de gravação são retomadas quando espaço livre adicional se torna disponível para o LUN ou namespace.

  Se a alocação de espaço não estiver ativada, quando um LUN ou namespace ficar sem espaço, todas as operações de e/S falharão e o LUN ou namespace for colocado off-line; o problema de espaço deve ser resolvido para retomar as operações normais. A nova digitalização de dispositivos LUN também pode ser necessária no host para restaurar caminhos e dispositivos para um estado operacional.

- Um host pode executar operações SCSI ou NVMe `UNMAP` (às vezes chamadas `TRIM`). As operações DE DESMAPEAMENTO permitem que um host identifique blocos de dados que não são mais necessários porque eles não contêm mais dados válidos. A identificação normalmente acontece após a exclusão do arquivo. O sistema de armazenamento pode então desalocar esses blocos de dados para que o espaço possa ser consumido em outro lugar. Essa realocação melhora significativamente a eficiência geral de armazenamento, especialmente com sistemas de arquivos que têm alta rotatividade de dados.

Antes de começar

A ativação da alocação de espaço requer uma configuração de host que possa lidar corretamente com erros de alocação de espaço quando uma gravação não pode ser concluída. A utilização de SCSI ou NVMe `UNMAP` requer uma configuração que possa usar o provisionamento de bloco lógico conforme definido no padrão

SCSI SBC-3.

Os hosts a seguir atualmente oferecem suporte a thin Provisioning quando você ativa a alocação de espaço:

- Citrix XenServer 6,5 e posterior
- VMware ESXi 5,0 e posterior
- Kernel Oracle Linux 6,2 UEK e posterior
- Red Hat Enterprise Linux 6,2 e posterior
- SUSE Linux Enterprise Server 11 e posterior
- Solaris 11,1 e posterior
- Windows

Sobre esta tarefa

Quando você atualiza seu cluster para o ONTAP 9.15,1 ou posterior, a configuração de alocação de espaço para todos os LUNs criados antes da atualização de software permanece a mesma após a atualização, independentemente do tipo de host. Por exemplo, se um LUN foi criado no ONTAP 9.13,1 para um host VMware com alocação de espaço desativada, a alocação de espaço nesse LUN permanecerá desativada após a atualização para o ONTAP 9.15,1.

Passos

1. Ativar alocação de espaço:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. Verifique se a alocação de espaço está ativada:

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Verifique se a alocação de espaço está ativada no sistema operacional do host.

> Algumas configurações de host, incluindo algumas versões do VMware ESXi, podem reconhecer automaticamente a alteração de configuração e não exigem intervenção do usuário. Outras configurações podem exigir uma nova digitalização do dispositivo. Alguns sistemas de arquivos e gerenciadores de volume podem exigir configurações específicas adicionais para habilitar a recuperação de espaço usando `SCSI UNMAP`o . A reinstalação de sistemas de arquivos ou uma reinicialização total do sistema operacional pode ser necessária. Consulte a documentação do seu host específico para obter orientação.

Configuração de host para hosts NVMe posteriores e VMware ESXi 8.x

Se você tiver um host VMware executando o ESXi 8.x ou posterior com o protocolo NVMe, depois de ativar a alocação de espaço no ONTAP, execute as etapas a seguir nos hosts.

Passos

1. No seu anfitrião ESXi, verifique se o DSM está desativado:

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   O valor esperado é 0.

2. Ativar o NVMe DSM:

   ```
   esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
   ```

3. Verifique se o DSM está ativado:

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   O valor esperado é 1.

Links relacionados

Saiba mais "Configuração de host NVMe-of para ESXi 8.x com ONTAP"sobre o .

Combinações recomendadas de volume e arquivo ou configuração LUN

Visão geral das combinações recomendadas de volume e arquivo ou configuração LUN

Existem combinações específicas de configurações de FlexVol volume e arquivo ou LUN que você pode usar, dependendo dos requisitos de aplicação e administração. Compreender os benefícios e os custos dessas combinações pode ajudá-lo a determinar a combinação certa de configuração de volume e LUN para o seu ambiente.

As seguintes combinações de configuração de volume e LUN são recomendadas:

- Arquivos ou LUNs com espaço reservado com provisionamento de volume espesso
- LUNs ou arquivos não reservados ao espaço com provisionamento de thin volumes
- Arquivos ou LUNs com espaço reservado com provisionamento de volume semi-espesso

Você pode usar o thin Provisioning SCSI em seus LUNs em conjunto com qualquer uma dessas combinações de configuração.

Arquivos ou LUNs com espaço reservado com provisionamento de volume espesso

Benefícios:

- Todas as operações de gravação dentro de arquivos reservados ao espaço são garantidas; elas não falharão devido a espaço insuficiente.
- Não há restrições quanto à eficiência de storage e às tecnologias de proteção de dados no volume.

Custos e limitações:

- Espaço suficiente deve ser separado do agregado na frente para suportar o volume provisionado thickly.
- O espaço igual a duas vezes o tamanho do LUN é alocado do volume no momento da criação do LUN.

LUNs ou arquivos não reservados ao espaço com provisionamento de thin volumes

Benefícios:

- Não há restrições quanto à eficiência de storage e às tecnologias de proteção de dados no volume.
- O espaço é alocado apenas como é usado.

Custos e restrições:

- As operações de gravação não são garantidas; elas podem falhar se o volume ficar sem espaço livre.
- Você deve gerenciar o espaço livre no agregado de forma eficaz para evitar que o agregado fique sem espaço livre.

Arquivos ou LUNs com espaço reservado com provisionamento de volume semi-espesso

Benefícios:

Há menos espaço reservado antes do que para o provisionamento de volume espesso, e ainda é fornecida uma garantia de gravação melhor esforço.

Custos e restrições:

- Operações de gravação podem falhar com essa opção.

  Você pode mitigar esse risco equilibrando adequadamente o espaço livre no volume em relação à volatilidade dos dados.

- Não é possível confiar na retenção de objetos de proteção de dados, como cópias Snapshot, arquivos FlexClone e LUNs.
- Você não pode usar os recursos de eficiência de storage de compartilhamento de bloco do ONTAP que não podem ser excluídos automaticamente, incluindo deduplicação, compactação e descarregamento de cópias/ODX.

Determine a combinação correta de volume e configuração LUN para o seu ambiente

Responder a algumas perguntas básicas sobre o seu ambiente pode ajudá-lo a determinar a melhor configuração de FlexVol volume e LUN para o seu ambiente.

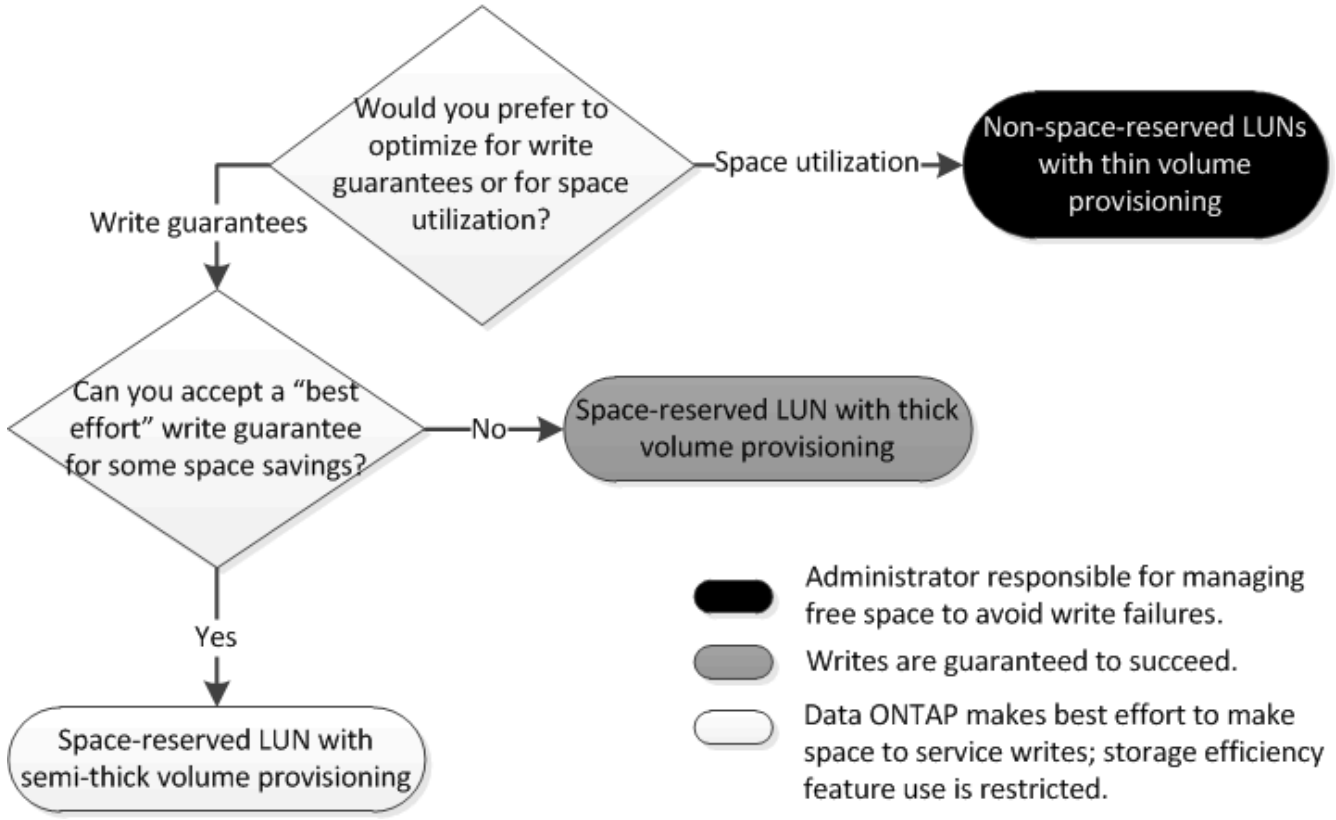
Sobre esta tarefa

Você pode otimizar as configurações de LUN e volume para a máxima utilização do storage ou para a segurança das garantias de gravação. Com base nos requisitos de utilização do storage e na capacidade de monitorar e reabastecer o espaço livre rapidamente, é necessário determinar os volumes de FlexVol volume e LUN apropriados para sua instalação.

Não é necessário um volume separado para cada LUN.

Passo

1. Use a seguinte árvore de decisão para determinar a melhor combinação de volume e configuração LUN para o seu ambiente:



Calcule a taxa de crescimento de dados para LUNs

Você precisa saber a taxa com que seus dados LUN estão crescendo ao longo do tempo para determinar se você deve usar LUNs com espaço reservado ou LUNs não reservados.

Sobre esta tarefa

Se você tiver uma taxa consistente de crescimento de dados, as LUNs com espaço reservado podem ser a melhor opção para você. Se você tiver uma taxa baixa de crescimento de dados, considere LUNs não reservados para espaço.

Você pode usar ferramentas como o OnCommand Insight para calcular a taxa de crescimento de dados ou calculá-la manualmente. As etapas a seguir são para cálculo manual.

Passos

1. Configure um LUN com espaço reservado.
2. Monitorize os dados no LUN durante um período de tempo definido, como uma semana.

   Certifique-se de que seu período de monitoramento é longo o suficiente para formar uma amostra representativa de aumentos regulares no crescimento de dados. Por exemplo, é possível que você tenha uma grande quantidade de crescimento de dados consistentemente no final de cada mês.

3. Todos os dias, Registre em GB quanto seus dados crescem.
4. No final do período de monitoramento, adicione os totais de cada dia juntos e divida pelo número de dias no período de monitoramento.

   Este cálculo produz a sua taxa média de crescimento.

Exemplo

Neste exemplo, você precisa de um LUN de 200 GB. Você decide monitorar o LUN por uma semana e Registrar as seguintes alterações diárias de dados:

- Domingo: 20 GB
- Segunda-feira: 18 GB
- Terça-feira: 17 GB
- Quarta-feira: 20 GB
- Quinta-feira: 20 GB
- Sexta-feira: 23 GB
- Sábado: 22 GB

Neste exemplo, sua taxa de crescimento é (20-18-17-20-20-23-22) / 7 é de 20 GB por dia.

Definições de configuração para ficheiros reservados ao espaço ou LUNs com volumes provisionados de espessura

Essa combinação de configuração de FlexVol volume e arquivo ou LUN permite usar tecnologias de eficiência de storage e não exige que você monitore ativamente o espaço livre, pois há espaço suficiente alocado inicialmente.

As configurações a seguir são necessárias para configurar um arquivo ou LUN com espaço reservado em um volume usando provisionamento espesso:

Definição do volume	Valor
Garantia	Volume
Reserva fracionária	100
Reserva do Snapshot	Qualquer
snapshot Autodelete	Opcional
Crescimento automático	Opcional; se ativado, o espaço livre agregado deve ser monitorado ativamente.

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Ativado

Configurações para arquivos não reservados ao espaço ou LUNs com volumes provisionados com thin

Essa combinação de configuração de FlexVol volume e arquivo ou LUN exige que a menor quantidade de storage seja alocada antes, mas requer gerenciamento ativo de espaço livre para evitar erros devido à falta de espaço.

As seguintes configurações são necessárias para configurar um LUN ou arquivos não reservados ao espaço em um volume provisionado com thin:

Definição do volume	Valor
Garantia	Nenhum
Reserva fracionária	0
Reserva do Snapshot	Qualquer
snapshot Autodelete	Opcional
Crescimento automático	Opcional

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Desativado

Considerações adicionais

Quando o volume ou agregado ficar sem espaço, as operações de gravação no arquivo ou LUN podem falhar.

Se você não quiser monitorar ativamente o espaço livre tanto para o volume quanto para o agregado, ative o crescimento automático para o volume e defina o tamanho máximo para o volume como o tamanho do agregado. Nessa configuração, você deve monitorar ativamente o espaço livre agregado, mas não precisa monitorar o espaço livre no volume.

Configurações para arquivos reservados ao espaço ou LUNs com provisionamento de volume semi-espesso

Essa combinação de configuração de FlexVol volume e arquivo ou LUN requer menos storage para ser alocado antes do que a combinação totalmente provisionada, mas impõe restrições às tecnologias de eficiência que você pode usar para o volume. As substituições são cumpridas com o melhor esforço para essa combinação de configuração.

As configurações a seguir são necessárias para configurar um LUN com espaço reservado em um volume usando provisionamento semi-espesso:

Definição do volume	Valor
Garantia	Volume
Reserva fracionária	0
Reserva do Snapshot	0

Definição do volume	Valor
snapshot Autodelete	On, com um nível de compromisso de destruir, uma lista de destruir que inclui todos os objetos, o gatilho definido para volume e todos os LUNs e arquivos FlexClone FlexClone ativados para exclusão automática.
Crescimento automático	Opcional; se ativado, o espaço livre agregado deve ser monitorado ativamente.

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Ativado

Restrições tecnológicas

Você não pode usar as seguintes tecnologias de eficiência de storage de volume para essa combinação de configuração:

- Compactação
- Deduplicação
- Descarregar cópias ODX e FlexClone
- LUNs e arquivos FlexClone do FlexClone não marcados para exclusão automática (clones ativos)
- Subficheiros FlexClone
- Descarregar ODX/Copy

Considerações adicionais

Os seguintes fatos devem ser considerados ao empregar esta combinação de configuração:

- Quando o volume compatível com o LUN é executado com pouco espaço, os dados de proteção (LUNs e arquivos FlexClone, cópias Snapshot) são destruídos.
- As operações de gravação podem ter tempo limite e falhar quando o volume ficar sem espaço livre.

A compactação é ativada por padrão para plataformas AFF. Você deve desativar explicitamente a compactação para qualquer volume para o qual deseja usar o provisionamento semi-espesso em uma plataforma AFF.

Proteção de dados SAN

Visão geral dos métodos de proteção de dados em ambientes SAN

Você pode proteger seus dados fazendo cópias deles para que fiquem disponíveis para restauração em caso de exclusão acidental, falhas no aplicativo, corrupção de dados ou desastre. Dependendo das suas necessidades de proteção e backup de dados, o ONTAP oferece uma variedade de métodos que permitem proteger seus dados.

Sincronização ativa do SnapMirror

A partir da disponibilidade geral no ONTAP 9.9,1, fornece objetivo de tempo de recuperação zero (rto zero) ou failover transparente de aplicações (TAF) para permitir o failover automático de aplicações essenciais aos negócios em ambientes SAN. O SnapMirror active Sync requer a instalação do ONTAP Mediator 1,2 em uma configuração com dois clusters AFF ou dois clusters All-Flash SAN Array (ASA).

"Sincronização ativa do SnapMirror"

Cópia Snapshot

Permite criar, agendar e manter, manualmente ou automaticamente, vários backups dos LUNs. As cópias snapshot usam apenas uma quantidade mínima de espaço de volume adicional e não têm custo de performance. Se seus dados LUN forem modificados ou excluídos acidentalmente, esses dados poderão ser restaurados de forma fácil e rápida a partir de uma das cópias Snapshot mais recentes.

FlexClone LUNs (é necessária licença FlexClone)

Fornece cópias graváveis e pontuais de outro LUN em um volume ativo ou em uma cópia Snapshot. Um clone e seu pai podem ser modificados independentemente sem afetar um ao outro.

SnapRestore (licença necessária)

Permite realizar uma recuperação de dados rápida, com uso eficiente de espaço e sob solicitação de cópias Snapshot em um volume inteiro. Você pode usar o SnapRestore para restaurar um LUN para um estado preservado anterior sem reiniciar o sistema de armazenamento.

Cópias espelhadas de proteção de dados (é necessária licença SnapMirror)

Fornece recuperação assíncrona de desastres, permitindo que você crie periodicamente cópias Snapshot de dados em seu volume, copie essas cópias Snapshot em uma rede local ou de área ampla para um volume de parceiro, geralmente em outro cluster e retenha essas cópias Snapshot. A cópia espelhada no volume do parceiro fornece disponibilidade e restauração rápidas dos dados a partir do momento da última cópia Snapshot, se os dados no volume de origem estiverem corrompidos ou perdidos.

Backups do SnapVault (é necessária licença SnapMirror)

Fornece retenção eficiente de backups a longo prazo e storage. Os relacionamentos do SnapVault permitem que você faça backup de cópias Snapshot selecionadas de volumes para um volume de destino e retenha os backups.

Se você conduzir backups em fita e operações de arquivamento, poderá executá-los nos dados que já tiverem backup no volume secundário do SnapVault.

SnapDrive para Windows ou UNIX (é necessária licença SnapDrive)

Configura o acesso a LUNs, gerencia LUNs e gerencia cópias Snapshot do sistema de storage diretamente de hosts Windows ou UNIX.

Backup e recuperação em fita nativa

O suporte para a maioria das unidades de fita existentes está incluído no ONTAP, bem como um método para que os fornecedores de fita adicionem suporte dinâmico a novos dispositivos. O ONTAP também suporta o protocolo de fita magnética remota (RMT), permitindo backup e recuperação para qualquer sistema capaz.

Informações relacionadas

"Documentação do NetApp: SnapDrive para UNIX"

"Documentação do NetApp: SnapDrive para Windows (versões atuais)"

"Proteção de dados usando backup em fita"

Efeito da movimentação ou cópia de um LUN em cópias Snapshot

Efeito da movimentação ou cópia de um LUN na visão geral das cópias Snapshot

As cópias snapshot são criadas no nível do volume. Se você copiar ou mover um LUN para um volume diferente, a política de cópia Snapshot da voluna de destino será aplicada ao volume copiado ou movido. Se as cópias Snapshot não estiverem estabelecidas para o volume de destino, as cópias Snapshot não serão criadas do LUN movido ou copiado.

Restaure um único LUN a partir de uma cópia Snapshot

Você pode restaurar um único LUN de uma cópia Snapshot sem restaurar todo o volume que contém o único LUN. Você pode restaurar o LUN no lugar ou para um novo caminho no volume. A operação restaura apenas o único LUN sem afetar outros arquivos ou LUNs no volume. Você também pode restaurar arquivos com streams.

O que você vai precisar

- Você deve ter espaço suficiente no volume para concluir a operação de restauração:
  - Se você estiver restaurando um LUN com espaço reservado em que a reserva fracionária seja de 0%, será necessário uma vez o tamanho do LUN restaurado.
  - Se você estiver restaurando um LUN com espaço reservado em que a reserva fracionária seja de 100%, será necessário duas vezes o tamanho do LUN restaurado.
  - Se você estiver restaurando um LUN não reservado com espaço, você só precisará do espaço real usado para o LUN restaurado.
- Uma cópia Snapshot do LUN de destino deve ter sido criada.

  Se a operação de restauração falhar, o LUN de destino pode ser truncado. Nesses casos, você pode usar a cópia Snapshot para evitar a perda de dados.

- Uma cópia Snapshot do LUN de origem deve ter sido criada.

  Em casos raros, a restauração LUN pode falhar, deixando o LUN de origem inutilizável. Se isso ocorrer, você pode usar a cópia Snapshot para retornar o LUN ao estado imediatamente antes da tentativa de restauração.

- O LUN de destino e o LUN de origem têm de ter o mesmo tipo de SO.

  Se o LUN de destino tiver um tipo de SO diferente do LUN de origem, o anfitrião poderá perder o acesso aos dados ao LUN de destino após a operação de restauro.

Passos

1. A partir do host, pare todo o acesso do host ao LUN.
2. Desmonte o LUN em seu host para que o host não possa acessar o LUN.
3. Desmapear o LUN:

   `lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

4. Determine a cópia Snapshot para a qual deseja restaurar o LUN:

   `volume snapshot show -vserver vserver_name -volume volume_name`

5. Crie uma cópia Snapshot do LUN antes de restaurar o LUN:

   `volume snapshot create -vserver vserver_name -volume volume_name -snapshot snapshot_name`

6. Restaure o LUN especificado em um volume:

   `volume snapshot restore-file -vserver vserver_name -volume volume_name -snapshot snapshot_name -path lun_path`

7. Siga os passos apresentados no ecrã.
8. Se necessário, coloque o LUN online:

   `lun modify -vserver vserver_name -path lun_path -state online`

9. Se necessário, remapear o LUN:

   `lun mapping create -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

10. Do host, remonte o LUN.
11. A partir do host, reinicie o acesso ao LUN.

Restaurar todos os LUNs em um volume a partir de uma cópia Snapshot

Você pode usar `volume snapshot restore` o comando para restaurar todos os LUNs em um volume especificado a partir de uma cópia Snapshot.

Passos

1. No host, interrompa todo o acesso do host aos LUNs.

   Usar o SnapRestore sem interromper todo o acesso do host aos LUNs no volume pode causar corrupção de dados e erros do sistema.

2. Desmonte os LUNs nesse host para que o host não possa acessar os LUNs.
3. Desmapear os LUNs:

   `lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

4. Determine a cópia Snapshot para a qual você deseja restaurar o volume:

   `volume snapshot show -vserver vserver_name -volume volume_name`

5. Altere a configuração de privilégio para avançado:

   `set -privilege advanced`

6. Restaure seus dados:

   `volume snapshot restore -vserver vserver_name -volume volume_name -snapshot snapshot_name`

7. Siga as instruções apresentadas no ecrã.
8. Remapear os LUNs:

   `lun mapping create -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

9. Verifique se os LUNs estão online:

   `lun show -vserver vserver_name -path lun_path -fields state`

10. Se os LUNs não estiverem online, coloque-os online:

    `lun modify -vserver vserver_name -path lun_path -state online`

11. Altere a configuração de privilégios para admin:

    `set -privilege admin`

12. No host, remonte seus LUNs.
13. No host, reinicie o acesso aos LUNs.

Exclua uma ou mais cópias Snapshot existentes de um volume

Você pode excluir manualmente uma ou mais cópias Snapshot existentes do volume. Você pode querer fazer isso se precisar de mais espaço em seu volume.

Passos

1. Use o `volume snapshot show` comando para verificar quais cópias snapshot você deseja excluir.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. Use o `volume snapshot delete` comando para excluir cópias Snapshot.

Se você quiser…	Digite este comando…
Excluir uma única cópia Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name`*
Exclua várias cópias Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name1`*`[,`*`snapshot_name2`*`,…]`
Excluir todas as cópias Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot *`

O exemplo a seguir exclui todas as cópias Snapshot no volume vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *

10 entries were acted on.
```

Use LUNs do FlexClone para proteger seus dados

Use LUNs FlexClone para proteger a visão geral dos dados

Um LUN FlexClone é uma cópia gravável e pontual de outro LUN em um volume ativo ou

em uma cópia Snapshot. O clone e seu pai podem ser modificados independentemente sem afetar um ao outro.

Um LUN FlexClone compartilha espaço inicialmente com seu LUN pai. Por padrão, o LUN FlexClone herda o atributo espaço reservado do LUN pai. Por exemplo, se o LUN pai não for reservado com espaço, o LUN FlexClone também não é reservado com espaço por padrão. No entanto, você pode criar um LUN FlexClone não reservado com espaço a partir de um pai que seja um LUN reservado com espaço.

Quando você clonar um LUN, o compartilhamento de bloco ocorre em segundo plano e não é possível criar uma cópia Snapshot de volume até que o compartilhamento de bloco seja concluído.

Tem de configurar o volume para ativar a função de eliminação automática LUN FlexClone com o `volume snapshot autodelete modify` comando. Caso contrário, se você quiser que os LUNs do FlexClone sejam excluídos automaticamente, mas o volume não estiver configurado para a exclusão automática do FlexClone, nenhum dos LUNs do FlexClone será excluído.

Quando você cria um LUN FlexClone, a função de exclusão automática FlexClone LUN é desativada por padrão. Você deve ativá-lo manualmente em cada LUN FlexClone antes que esse LUN FlexClone possa ser excluído automaticamente. Se você estiver usando o provisionamento de volume semi-espesso e quiser a garantia de gravação "melhor esforço" fornecida por essa opção, você deve disponibilizar *All* FlexClone LUNs para exclusão automática.

> Quando você cria um LUN FlexClone a partir de uma cópia Snapshot, o LUN é automaticamente dividido da cópia Snapshot usando um processo em segundo plano com uso eficiente de espaço para que o LUN não continue a depender da cópia Snapshot ou consumir nenhum espaço adicional. Se esta divisão em segundo plano não tiver sido concluída e esta cópia Snapshot for automaticamente eliminada, esse LUN FlexClone será eliminado mesmo que tenha desativado a função de eliminação automática do FlexClone para esse LUN FlexClone. Depois que a divisão em segundo plano estiver concluída, o LUN FlexClone não será excluído mesmo que essa cópia Snapshot seja excluída.

Informações relacionadas

"Gerenciamento de storage lógico"

Razões para usar LUNs FlexClone

Você pode usar LUNs do FlexClone para criar várias cópias de leitura/gravação de um LUN.

Você pode querer fazer isso pelas seguintes razões:

- Você precisa criar uma cópia temporária de um LUN para fins de teste.
- Você precisa disponibilizar uma cópia de seus dados para usuários adicionais sem dar acesso aos dados de produção.
- Você deseja criar um clone de um banco de dados para operações de manipulação e projeção, preservando os dados originais de uma forma inalterada.
- Você deseja acessar um subconjunto específico de dados de um LUN (um volume lógico específico ou sistema de arquivos em um grupo de volumes ou um arquivo específico ou conjunto de arquivos em um sistema de arquivos) e copiá-lo para o LUN original, sem restaurar o restante dos dados no LUN original. Isso funciona em sistemas operacionais que suportam a montagem de um LUN e um clone do LUN ao mesmo tempo. O SnapDrive para UNIX suporta isso com o `snap connect` comando.

- Você precisa de vários hosts de inicialização SAN com o mesmo sistema operacional.

Como um FlexVol volume pode recuperar espaço livre com a configuração de transferência de dados

Pode ativar a definição de FlexVol volume para eliminar automaticamente ficheiros FlexClone e LUNs FlexClone. Ao ativar o serviço de correio eletrónico, pode recuperar uma quantidade alvo de espaço livre no volume quando um volume estiver quase cheio.

Você pode configurar um volume para começar a excluir automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminuir abaixo de um determinado valor limite e parar automaticamente de excluir clones quando uma quantidade de espaço livre no volume for recuperada. Embora não seja possível especificar o valor de limite que inicia a exclusão automática de clones, você pode especificar se um clone é elegível para exclusão e especificar a quantidade de espaço livre de destino para um volume.

Um volume exclui automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminui abaixo de um determinado limite e quando *ambos* dos seguintes requisitos são atendidos:

- A funcionalidade de autodelete está ativada para o volume que contém os arquivos FlexClone e LUNs FlexClone.

  Você pode ativar a capacidade de transferência de um FlexVol volume usando o `volume snapshot autodelete modify` comando. Você deve definir o `-trigger` parâmetro para `volume` ou `snap_reserve` para que um volume exclua automaticamente arquivos FlexClone e LUNs FlexClone.

- A funcionalidade de configuração do sistema de áudio e vídeo é habilitada para os LUNs FlexClone e FlexClone.

  Você pode ativar o arquivo FlexClone ou FlexClone LUN usando o `file clone create` comando com o `-autodelete` parâmetro. Como resultado, você pode preservar certos arquivos FlexClone e LUNs FlexClone, desativando o serviço de seleção de clones e garantindo que outras configurações de volume não substituam a configuração de clone.

Configure um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone

Pode ativar um FlexVol volume para eliminar automaticamente ficheiros FlexClone e LUNs FlexClone com o sistema de gestão de dados em curso ativado quando o espaço livre no volume diminui abaixo de um determinado limite.

O que você vai precisar

- O FlexVol volume deve conter arquivos FlexClone e LUNs FlexClone e estar online.
- O FlexVol volume não deve ser um volume somente leitura.

Passos

1. Ative a exclusão automática de arquivos FlexClone e LUNs FlexClone no FlexVol volume usando o `volume snapshot autodelete modify` comando.
   - Para o `-trigger` parâmetro, pode especificar `volume` ou `snap_reserve`.
   - Para o `-destroy-list` parâmetro, você deve sempre especificar `lun_clone,file_clone`, independentemente de você querer excluir apenas um tipo de clone. O exemplo a seguir mostra como você pode ativar o volume vol1 para acionar a exclusão automática de arquivos FlexClone e LUNs

FlexClone para recuperação de espaço até que 25% do volume consista em espaço livre:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

> Ao ativar volumes FlexVol para exclusão automática, se você definir o valor `-commitment` do parâmetro como `destroy`, todos os arquivos FlexClone e LUNs FlexClone com o `-autodelete` parâmetro definido como `true` poderão ser excluídos quando o espaço livre no volume diminuir abaixo do valor de limite especificado. No entanto, os arquivos FlexClone e LUNs FlexClone com o `-autodelete` parâmetro definido como `false` não serão excluídos.

2. Verifique se a exclusão automática de arquivos FlexClone e LUNs FlexClone está ativada no FlexVol volume usando o `volume snapshot autodelete show` comando.

   O exemplo a seguir mostra que o volume vol1 está habilitado para exclusão automática de arquivos FlexClone e LUNs FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
            Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)*
    Target Free Space: 25%
              Trigger: volume
     Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. Certifique-se de que o serviço de correio eletrónico está ativado para os ficheiros FlexClone e LUNs FlexClone no volume que pretende eliminar, executando as seguintes etapas:

   a. Ative a exclusão automática de um arquivo FlexClone específico ou LUN FlexClone usando o `volume file clone autodelete` comando.

      Você pode forçar um arquivo FlexClone específico ou LUN FlexClone a ser automaticamente excluído usando o `volume file clone autodelete` comando com o `-force` parâmetro.

      O exemplo a seguir mostra que a exclusão automática do FlexClone LUN lun1_clone contido no volume vol1 está ativada:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

Você pode ativar o arquivo FlexClone e LUNs do FlexClone.

b. Verifique se o arquivo FlexClone ou FlexClone LUN está habilitado para exclusão automática usando o `volume file clone show-autodelete` comando.

O exemplo a seguir mostra que o FlexClone LUN lun1_clone está habilitado para exclusão automática:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone
Path: vol/vol1/lun1_clone

**Autodelete Enabled: true**
```

Para obter mais informações sobre como usar os comandos, consulte as respetivas páginas de manual.

Clonar LUNs de um volume ativo

É possível criar cópias dos LUNs clonando os LUNs no volume ativo. Esses LUNs FlexClone são cópias legíveis e graváveis dos LUNs originais no volume ativo.

> Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para clonar dados. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

O que você vai precisar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

Um LUN FlexClone reservado com espaço requer tanto espaço quanto o LUN pai reservado com espaço. Se o LUN FlexClone não tiver espaço reservado, você deve garantir que o volume tenha espaço suficiente para acomodar alterações no LUN FlexClone.

Passos

1. Você deve ter verificado que os LUNs não são mapeados para um iggroup ou são gravados antes de fazer o clone.
2. Use o `lun show` comando para verificar se o LUN existe.

```
lun show -vserver vs1
```

```
Vserver  Path                State     Mapped    Type      Size
-------- ------------------ --------- --------- -------- -------
vs1      /vol/vol1/lun1     online    unmapped  windows  47.07MB
```

3. Use o `volume file clone create` comando para criar o LUN FlexClone.

   ```
   volume file clone create -vserver vs1 -volume vol1 -source-path lun1
   -destination-path/lun1_clone
   ```

   Se você precisar que o LUN FlexClone esteja disponível para exclusão automática, inclua `-autodelete true`o . Se você estiver criando esse LUN FlexClone em um volume usando provisionamento semi-espesso, será necessário habilitar a exclusão automática para todos os LUNs FlexClone.

4. Use o `lun show` comando para verificar se você criou um LUN.

   ```
   lun show -vserver vs1
   ```

```
Vserver  Path                      State    Mapped   Type      Size
-------- ------------------------ -------- -------- -------- ------
vs1      /vol/volX/lun1           online   unmapped windows  47.07MB
vs1      /vol/volX/lun1_clone     online   unmapped windows  47.07MB
```

Criar LUNs FlexClone a partir de uma cópia Snapshot em um volume

Você pode usar uma cópia Snapshot no volume para criar cópias FlexClone dos LUNs. Cópias FlexClone de LUNs são legíveis e graváveis.

O que você vai precisar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

O LUN FlexClone herda o atributo de reservas de espaço do LUN pai. Um LUN FlexClone reservado com espaço requer tanto espaço quanto o LUN pai reservado com espaço. Se o LUN FlexClone não estiver reservado com espaço, o volume deverá ter espaço suficiente para acomodar alterações no clone.

Passos

1. Verifique se o LUN não está mapeado ou a ser gravado.
2. Crie uma cópia Snapshot do volume que contém os LUNs:

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

   Você deve criar uma cópia Snapshot (a cópia Snapshot de backup) do LUN que deseja clonar.

3. Crie o LUN FlexClone a partir da cópia Snapshot:

   ```
   file clone create -vserver vserver_name -volume volume_name -source-path
   ```

source_path -snapshot-name *snapshot_name* -destination-path *destination_path*

Se você precisar que o LUN FlexClone esteja disponível para exclusão automática, inclua `-autodelete true`o . Se você estiver criando esse LUN FlexClone em um volume usando provisionamento semi-espesso, será necessário habilitar a exclusão automática para todos os LUNs FlexClone.

4. Verifique se o LUN FlexClone está correto:

   `lun show -vserver *vserver_name*`

```
Vserver Path                      State    Mapped    Type     Size
------- ----------------------    -------- --------- -------- -------
vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
```

Impedir a eliminação automática de um ficheiro FlexClone ou LUN FlexClone

Se você configurar um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone, qualquer clone que atenda aos critérios especificados poderá ser excluído. Se você tiver arquivos FlexClone ou LUNs FlexClone específicos que deseja preservar, poderá excluí-los do processo de exclusão automática do FlexClone.

Antes de começar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

Quando você cria um arquivo FlexClone ou LUN FlexClone, por padrão, a configuração de ciclo de vida para o clone é desativada. Os arquivos do FlexClone e os LUNs do FlexClone com o recurso de configuração de ciclo de vida desativado são preservados quando você configura um FlexVol volume para excluir automaticamente clones para recuperar espaço no volume.

> Se você definir o `commitment` nível no volume como `try` ou `disrupt`, poderá preservar individualmente arquivos FlexClone ou LUNs FlexClone específicos desativando o modo de exibição de dados para esses clones. No entanto, se você definir o `commitment` nível no volume como `destroy` e as listas destruir incluir `lun_clone,file_clone`, a configuração de volume substituirá a configuração clone e todos os arquivos FlexClone e FlexClone LUNs poderão ser excluídos independentemente da configuração de ciclo de vida dos clones.

Passos

1. Evite que um arquivo FlexClone específico ou LUN FlexClone seja excluído automaticamente usando o `volume file clone autodelete` comando.

   O exemplo a seguir mostra como você pode desativar o FlexClone LUN lun1_clone contido no vol1:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

Um arquivo ou LUN FlexClone com o sistema de diagnóstico guiado por sintomas (FlexClone) desativado não pode ser excluído automaticamente para recuperar espaço no volume.

2. Verifique se o arquivo FlexClone ou FlexClone LUN está desabilitado usando o `volume file clone show-autodelete` comando.

   O exemplo a seguir mostra que o FlexClone lun lun1_clone é falso:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone Path:
vol/vol1/lun1_clone
                                                                Autodelete
Enabled: false
```

Configurar e usar backups do SnapVault em um ambiente SAN

Configure e use backups do SnapVault em uma visão geral do ambiente SAN

A configuração e o uso do SnapVault em um ambiente SAN são muito semelhantes à configuração e ao uso em um ambiente nas, mas a restauração de LUNs em um ambiente SAN requer alguns procedimentos especiais.

Os backups do SnapVault contêm um conjunto de cópias somente leitura de um volume de origem. Em um ambiente SAN, você sempre faz backup de volumes inteiros para o volume secundário do SnapVault, e não LUNs individuais.

O procedimento para criar e inicializar a relação SnapVault entre um volume primário que contém LUNs e um volume secundário que atua como um backup do SnapVault é idêntico ao procedimento usado com volumes FlexVol usados para protocolos de arquivo. Este procedimento é descrito em pormenor em "Proteção de dados".

É importante garantir que o backup de LUNs que estão sendo feitos estejam em um estado consistente antes que as cópias Snapshot sejam criadas e copiadas para o volume secundário do SnapVault. A automação da criação de cópias Snapshot com o SnapCenter garante que os LUNs de backup sejam completos e utilizáveis pela aplicação original.

Há três opções básicas para restaurar LUNs de um volume secundário do SnapVault:

- Você pode mapear um LUN diretamente do volume secundário do SnapVault e conetar um host ao LUN para acessar o conteúdo do LUN.

  O LUN é somente leitura e você pode mapear apenas a partir da cópia Snapshot mais recente no backup do SnapVault. Reservas persistentes e outros metadados LUN são perdidos. Se desejar, você pode usar um programa de cópia no host para copiar o conteúdo do LUN de volta para o LUN original, se ele ainda estiver acessível.

  O LUN tem um número de série diferente do LUN de origem.

- Você pode clonar qualquer cópia Snapshot no volume secundário do SnapVault para um novo volume de leitura-gravação.

  Em seguida, é possível mapear qualquer um dos LUNs no volume e conetar um host ao LUN para acessar o conteúdo do LUN. Se desejar, você pode usar um programa de cópia no host para copiar o conteúdo do LUN de volta para o LUN original, se ele ainda estiver acessível.

- Você pode restaurar todo o volume que contém o LUN de qualquer cópia Snapshot no volume secundário do SnapVault.

  A restauração de todo o volume substitui todos os LUNs e quaisquer arquivos no volume. Todos os novos LUNs criados desde a criação da cópia Snapshot são perdidos.

  Os LUNs retêm seu mapeamento, números de série, UUIDs e reservas persistentes.

Acesse uma cópia LUN somente leitura a partir de um backup do SnapVault

Você pode acessar uma cópia somente leitura de um LUN a partir da cópia Snapshot mais recente em um backup do SnapVault. O ID do LUN, o caminho e o número de série são diferentes do LUN de origem e devem primeiro ser mapeados. Reservas persistentes, mapeamentos de LUN e grupos não são replicados para o volume secundário do SnapVault.

O que você vai precisar

- A relação SnapVault deve ser inicializada e a cópia Snapshot mais recente no volume secundário do SnapVault deve conter o LUN desejado.
- A máquina virtual de storage (SVM) que contém o backup do SnapVault deve ter uma ou mais LIFs com o protocolo SAN desejado acessível a partir do host usado para acessar a cópia LUN.
- Se você planeja acessar cópias LUN diretamente do volume secundário do SnapVault, crie seus grupos no SnapVault SVM com antecedência.

  Você pode acessar um LUN diretamente do volume secundário do SnapVault sem precisar primeiro restaurar ou clonar o volume que contém o LUN.

Sobre esta tarefa

Se uma nova cópia Snapshot for adicionada ao volume secundário do SnapVault enquanto você tiver um LUN mapeado de uma cópia Snapshot anterior, o conteúdo do LUN mapeado será alterado. O LUN ainda é mapeado com os mesmos identificadores, mas os dados são retirados da nova cópia Snapshot. Se o tamanho do LUN mudar, alguns hosts detetarão automaticamente a alteração de tamanho; os hosts do Windows exigem uma nova varredura de disco para pegar qualquer alteração de tamanho.

Passos

1. Execute o `lun show` comando para listar os LUNs disponíveis no volume secundário do SnapVault.

   Neste exemplo, você pode ver os LUNs originais no volume primário srcvolA e as cópias no volume secundário do SnapVault dstvolB:

```
cluster::> lun show

Vserver   Path                State   Mapped   Type          Size
--------  ------------------  ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

2. Se o igrop para o host desejado ainda não existir no SVM que contém o volume secundário do SnapVault, execute o `igroup create` comando para criar um igrop.

   Este comando cria um grupo para um host do Windows que usa o protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. Execute o `lun mapping create` comando para mapear a cópia LUN desejada para o igroup.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

4. Conete o host ao LUN e acesse o conteúdo do LUN conforme desejado.

Restaure um único LUN a partir de um backup do SnapVault

Você pode restaurar um único LUN para um novo local ou para o local original. Você pode restaurar a partir de qualquer cópia Snapshot no volume secundário do SnapVault. Para restaurar o LUN para o local original, primeiro restaure-o para um novo local e, em seguida, copie-o.

O que você vai precisar

- A relação do SnapVault deve ser inicializada e o volume secundário do SnapVault deve conter uma cópia Snapshot apropriada para ser restaurada.
- A máquina virtual de storage (SVM) que contém o volume secundário do SnapVault deve ter uma ou mais LIFs com o protocolo SAN desejado que podem ser acessados pelo host usado para acessar a cópia LUN.
- Os grupos já devem existir no SnapVault SVM.

Sobre esta tarefa

O processo inclui a criação de um clone de volume de leitura e gravação a partir de uma cópia Snapshot no volume secundário do SnapVault. Você pode usar o LUN diretamente do clone ou, opcionalmente, copiar o conteúdo do LUN de volta para o local original do LUN.

O LUN no clone tem um caminho e um número de série diferentes do LUN original. Reservas persistentes não são retidas.

Passos

1. Execute o `snapmirror show` comando para verificar o volume secundário que contém o backup do SnapVault.

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

2. Execute o `volume snapshot show` comando para identificar a cópia Snapshot da qual você deseja restaurar o LUN.

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. Execute o `volume clone create` comando para criar um clone de leitura e gravação a partir da cópia Snapshot desejada.

   O clone de volume é criado no mesmo agregado que o backup do SnapVault. Deve haver espaço suficiente no agregado para armazenar o clone.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Execute o `lun show` comando para listar os LUNs no clone de volume.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

5. Se o igrop para o host desejado ainda não existir no SVM que contém o backup do SnapVault, execute o `igroup create` comando para criar um igrop.

   Este exemplo cria um grupo para um host do Windows que usa o protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Execute o `lun mapping create` comando para mapear a cópia LUN desejada para o igroup.

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Conete o host ao LUN e acesse o conteúdo do LUN, conforme desejado.

   O LUN é leitura-escrita e pode ser usado no lugar do LUN original. Como o número de série do LUN é diferente, o host o interpreta como um LUN diferente do original.

8. Use um programa de cópia no host para copiar o conteúdo do LUN de volta para o LUN original.

Restaurar todos os LUNs em um volume a partir de um backup do SnapVault

Se um ou mais LUNs em um volume precisarem ser restaurados a partir de um backup do SnapVault, você poderá restaurar todo o volume. A restauração do volume afeta todos os LUNs no volume.

O que você vai precisar

A relação do SnapVault deve ser inicializada e o volume secundário do SnapVault deve conter uma cópia Snapshot apropriada para ser restaurada.

Sobre esta tarefa

Restaurar um volume inteiro retorna o volume ao estado em que estava quando a cópia Snapshot foi feita. Se um LUN foi adicionado ao volume após a cópia Snapshot, esse LUN será removido durante o processo de

restauração.

Depois de restaurar o volume, os LUNs permanecem mapeados para os grupos para os quais foram mapeados pouco antes da restauração. O mapeamento LUN pode ser diferente do mapeamento no momento da cópia Snapshot. Reservas persistentes nas LUNs dos clusters de host são retidas.

Passos

1. Pare a e/S para todos os LUNs no volume.
2. Execute o `snapmirror show` comando para verificar o volume secundário que contém o volume secundário do SnapVault.

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

3. Execute o `volume snapshot show` comando para identificar a cópia Snapshot da qual você deseja restaurar.

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. Execute o `snapmirror restore` comando e especifique a `-source-snapshot` opção para especificar a cópia Snapshot a ser usada.

   O destino especificado para a restauração é o volume original para o qual você está restaurando.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Se você estiver compartilhando LUNs em um cluster de host, restaure as reservas persistentes nos LUNs dos hosts afetados.

Restaurar um volume a partir de uma cópia de segurança do SnapVault

No exemplo a seguir, o LUN chamado LUN_D foi adicionado ao volume depois que a cópia Snapshot foi criada. Depois de restaurar todo o volume da cópia Snapshot, lun_D não aparece mais.

Na `lun show` saída do comando, você pode ver os LUNs no volume primário srcvolA e as cópias somente leitura desses LUNs no volume secundário do SnapVault dstvolB. Não há cópia de lun_D no backup do SnapVault.

```
cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

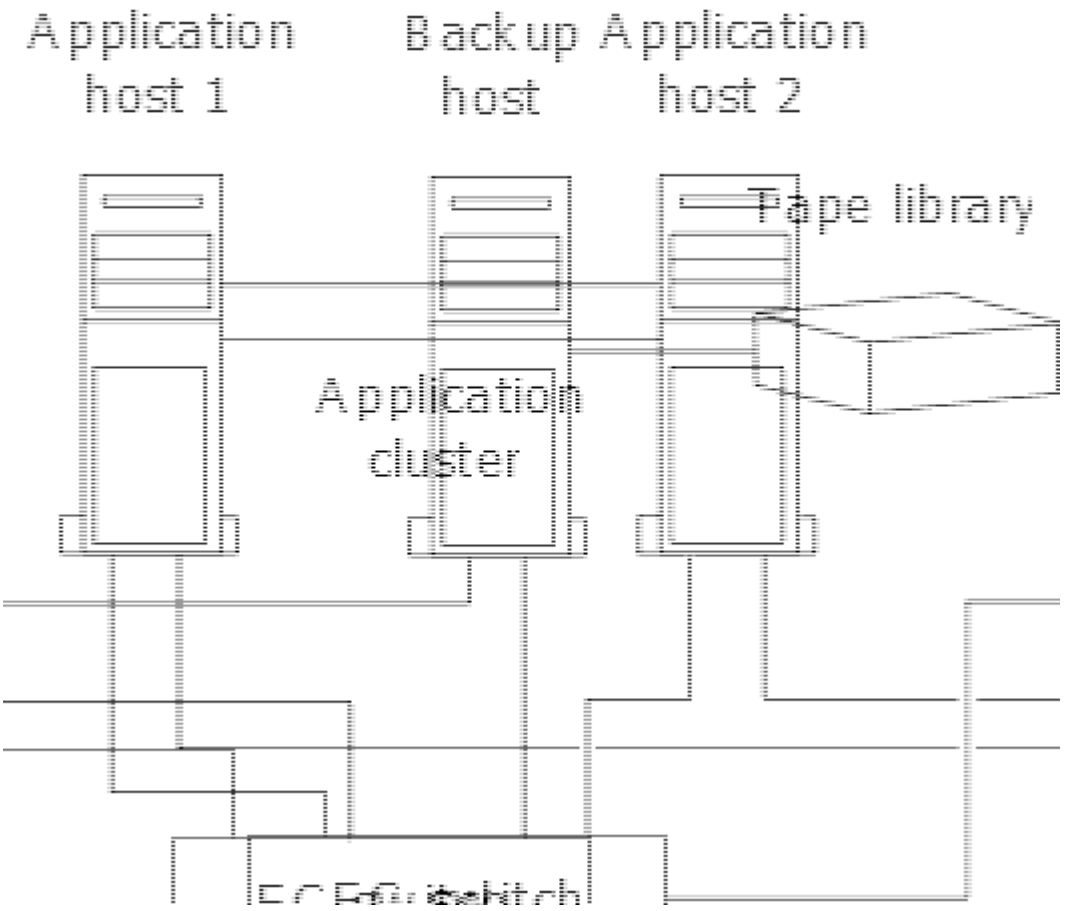
Depois que o volume é restaurado a partir do volume secundário do SnapVault, o volume de origem não contém mais lun_D. Não é necessário remapear novamente os LUNs no volume de origem após a restauração, pois eles ainda estão mapeados.

Como conetar um sistema de backup de host ao sistema de storage primário

É possível fazer backup de sistemas SAN na fita por meio de um host de backup separado para evitar a degradação da performance no host do aplicativo.

É imperativo que você mantenha os dados SAN e nas separados para fins de backup. A figura abaixo mostra a configuração física recomendada para um sistema de backup do host para o sistema de storage primário.

Você deve configurar volumes como somente SAN. Os LUNs podem ser confinados a um único volume ou os LUNs podem ser espalhados por vários volumes ou sistemas de armazenamento.



Os volumes em um host podem consistir em um único LUN mapeado a partir do sistema de armazenamento ou vários LUNs usando um gerenciador de volumes, como VxVM em sistemas HP-UX.

Faça backup de um LUN por meio de um sistema de backup de host

Você pode usar um LUN clonado de uma cópia Snapshot como dados de origem para o sistema de backup do host.

O que você vai precisar

Um LUN de produção deve existir e ser mapeado para um grupo que inclua o nome do nó WWPN ou iniciador do servidor de aplicativos. O LUN também deve ser formatado e acessível ao host

Passos

1. Salve o conteúdo dos buffers do sistema de arquivos host no disco.

   Você pode usar o comando fornecido pelo seu sistema operacional host ou usar o SnapDrive para Windows ou SnapDrive para UNIX. Você também pode optar por fazer desta etapa parte do script de pré-processamento de backup SAN.

2. Use o `volume snapshot create` comando para criar uma cópia Snapshot do LUN de produção.

   ```
   volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot
   -comment "Single snapshot" -foreground false
   ```

3. Use o `volume file clone create` comando para criar um clone do LUN de produção.

   ```
   volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot
   -name snap_vol3 -destination-path lun1_backup
   ```

4. Use o `lun igroup create` comando para criar um grupo que inclua o WWPN do servidor de backup.

   ```
   lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows
   -initiator 10:00:00:00:c9:73:5b:91
   ```

5. Use o `lun mapping create` comando para mapear o clone LUN que você criou na Etapa 3 para o host de backup.

   ```
   lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
   ```

   Você pode optar por fazer desta etapa parte do script de pós-processamento do aplicativo de backup SAN.

6. A partir do host, descubra o novo LUN e disponibilize o sistema de arquivos para o host.

   Você pode optar por fazer desta etapa parte do script de pós-processamento do aplicativo de backup SAN.

7. Faça backup dos dados no clone LUN do host de backup para fita usando seu aplicativo de backup SAN.
8. Use o `lun modify` comando para colocar o clone LUN off-line.

   ```
   lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
   ```

9. Utilize o `lun delete` para remover o clone LUN.

   ```
   lun delete -vserver vs3 -volume vol3 -lun lun1_backup
   ```

10. Use o `volume snapshot delete` comando para remover a cópia Snapshot.

    ```
    volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
    ```

Referência de configuração SAN

Visão geral da configuração SAN

Uma rede de área de storage (SAN) consiste em uma solução de storage conetada a hosts por meio de um protocolo de transporte SAN, como iSCSI ou FC. Você pode configurar sua SAN para que sua solução de armazenamento seja conetada aos hosts por meio de um ou mais switches. Se você estiver usando iSCSI, também poderá configurar sua SAN para que sua solução de armazenamento seja conetada diretamente ao host sem usar um switch.

Em uma SAN, vários hosts, usando sistemas operacionais diferentes, como Windows, Linux ou UNIX, podem acessar a solução de storage ao mesmo tempo. Você pode usar "Mapeamento LUN seletivo" e "portsets" para limitar o acesso aos dados entre os hosts e o armazenamento.

Para iSCSI, a topologia de rede entre a solução de armazenamento e os hosts é chamada de rede. Para FC, FC/NVMe e FCoE, a topologia de rede entre a solução de storage e os hosts é conhecida como malha. Para criar redundância, que o protege contra a perda de acesso aos dados, você deve configurar sua SAN com pares de HA em uma configuração de várias redes ou várias estruturas. Configurações que usam nós únicos ou redes/malhas únicas não são totalmente redundantes, portanto não são recomendadas.

Depois de configurar a SAN, pode "Provisionar storage para iSCSI ou FC"ou pode "Provisionar storage para FC/NVMe". Então você pode se conetar aos seus hosts para começar a prestar serviços de dados.

O suporte ao protocolo SAN varia de acordo com sua versão do ONTAP, sua plataforma e sua configuração. Para obter detalhes sobre sua configuração específica, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Informações relacionadas

- "Visão geral da administração DE SAN"
- "Configuração, suporte e limitações do NVMe"

Configurações iSCSI

Maneiras de configurar hosts SAN iSCSI

Você deve configurar sua configuração iSCSI com pares de alta disponibilidade (HA) que se conetam diretamente aos hosts SAN iSCSI ou que se conetam aos hosts por meio de um ou mais switches IP.

"Pares HA" São definidos como os nós de relatório para os caminhos Ativo/otimizado e Ativo/Unoptimized que serão usados pelos hosts para acessar os LUNs. Vários hosts, usando sistemas operacionais diferentes, como Windows, Linux ou UNIX, podem acessar o storage ao mesmo tempo. Os hosts exigem que uma solução de multipathing suportada que suporte ALUA seja instalada e configurada. Sistemas operacionais suportados e soluções multipathing podem ser verificados no "Ferramenta de Matriz de interoperabilidade do NetApp".

Em uma configuração de várias redes, há dois ou mais switches conetando os hosts ao sistema de armazenamento. As configurações de várias redes são recomendadas porque são totalmente redundantes. Em uma configuração de rede única, há um switch conetando os hosts ao sistema de armazenamento. As configurações de rede única não são totalmente redundantes.

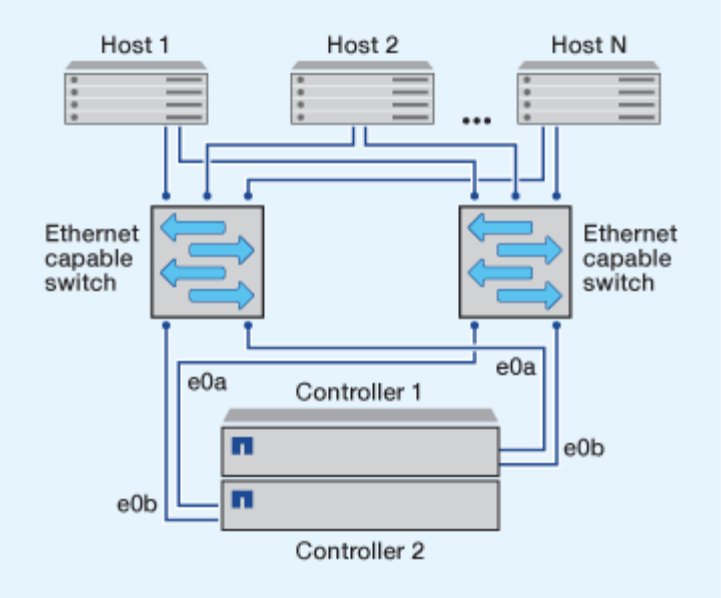
> "Configurações de nó único" não são recomendadas porque não fornecem a redundância necessária para dar suporte à tolerância de falhas e operações ininterruptas.

Informações relacionadas

- Saiba como "Mapeamento LUN seletivo (SLM)" limita os caminhos utilizados para acessar as LUNs de propriedade de um par de HA.
- Saiba mais "SAN LIFs"sobre .
- Saiba mais sobre o "Benefícios das VLANs no iSCSI".

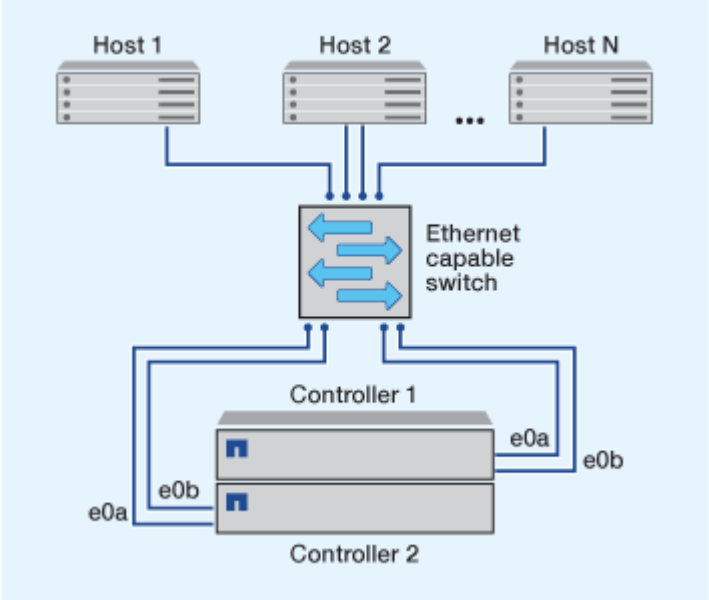
Configurações iSCSI de várias redes

Em configurações de par de HA com várias redes, dois ou mais switches conetam o par de HA a um ou mais hosts. Como existem vários switches, essa configuração é totalmente redundante.



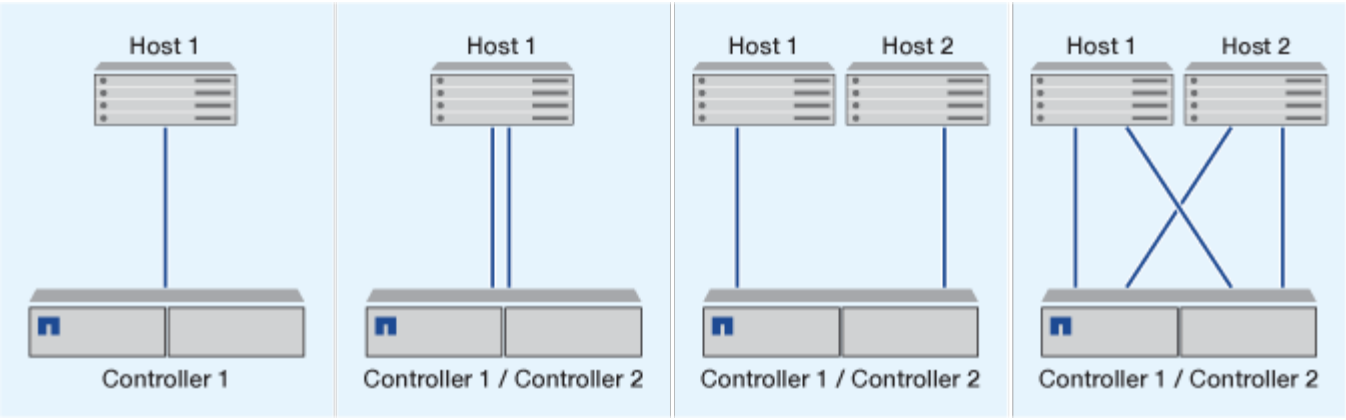
Configurações iSCSI de rede única

Nas configurações de par de HA de rede única, um switch conecta o par de HA a um ou mais hosts. Como há um único switch, essa configuração não é totalmente redundante.



Configuração iSCSI de ligação direta

Em uma configuração com conexão direta, um ou mais hosts são conetados diretamente aos controladores.



Benefícios de usar VLANs em configurações iSCSI

Uma VLAN consiste em um grupo de portas de switch agrupadas em um domínio de broadcast. Uma VLAN pode estar em um único switch ou pode abranger vários chassis de switch. As VLANs estáticas e dinâmicas permitem aumentar a segurança, isolar problemas e limitar os caminhos disponíveis na infraestrutura de rede IP.

Ao implementar VLANs em grandes infraestruturas de rede IP, você obtém os seguintes benefícios:

- Maior segurança.

  As VLANs permitem que você aproveite a infra-estrutura existente e ainda forneça segurança aprimorada, pois limitam o acesso entre diferentes nós de uma rede Ethernet ou uma SAN IP.

- Maior confiabilidade da rede Ethernet e da SAN IP ao isolar problemas.
- Redução do tempo de resolução de problemas limitando o espaço do problema.
- Redução do número de caminhos disponíveis para uma porta de destino iSCSI específica.
- Redução do número máximo de caminhos usados por um host.

  Ter muitos caminhos retarda os tempos de reconexão. Se um host não tiver uma solução multipathing, você poderá usar VLANs para permitir apenas um caminho.

VLANs dinâmicas

As VLANs dinâmicas são baseadas em endereços MAC. Você pode definir uma VLAN especificando o endereço MAC dos membros que deseja incluir.

As VLANs dinâmicas fornecem flexibilidade e não exigem mapeamento para as portas físicas onde o dispositivo está fisicamente conetado ao switch. Você pode mover um cabo de uma porta para outra sem reconfigurar a VLAN.

VLANs estáticas

As VLANs estáticas são baseadas em portas. O switch e a porta do switch são usados para definir a VLAN e seus membros.

As VLANs estáticas oferecem segurança aprimorada porque não é possível violar VLANs usando spoofing de controle de acesso de Mídia (MAC). No entanto, se alguém tiver acesso físico ao switch, substituir um cabo e reconfigurar o endereço de rede poderá permitir o acesso.

Em alguns ambientes, é mais fácil criar e gerenciar VLANs estáticas do que VLANs dinâmicas. Isso ocorre porque as VLANs estáticas exigem que somente o switch e o identificador de porta sejam especificados, em vez do endereço MAC de 48 bits. Além disso, você pode rotular intervalos de portas do switch com o identificador VLAN.

Configurações de FC

Maneiras de configurar hosts SAN FC e FC-NVMe

É recomendável configurar seus hosts SAN FC e FC-NVMe usando pares de HA e no mínimo dois switches. Isso fornece redundância nas camadas de malha e sistema de storage para dar suporte a tolerância de falhas e operações ininterruptas. Você não pode conectar diretamente hosts SAN FC ou FC-NVMe a pares de HA sem usar um switch.

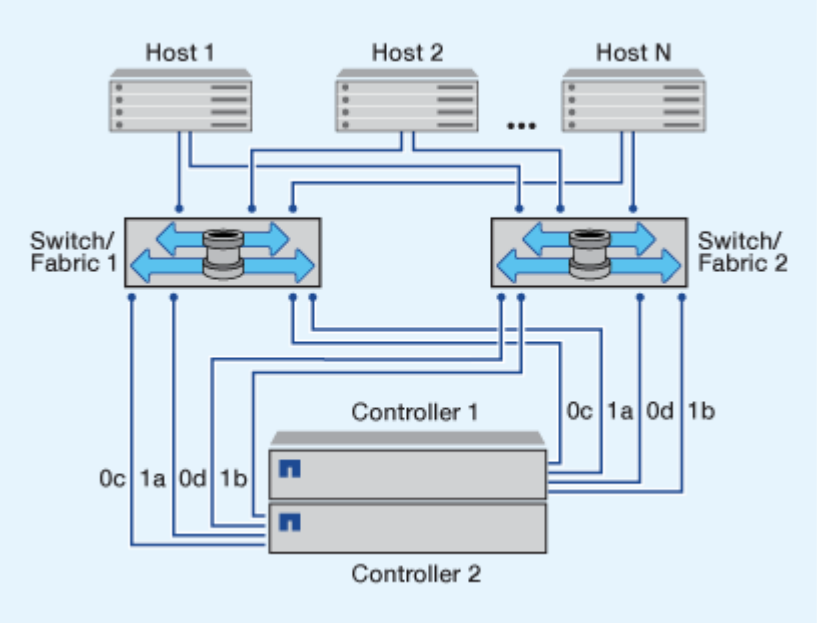
Cascata, malha parcial, malha completa, borda central e tecidos diretor são todos métodos padrão do setor de conexão de switches FC a uma malha e todos são compatíveis. O uso de malhas de switch FC heterogêneas não é suportado, exceto no caso de switches blade incorporados. Exceções específicas estão listadas no "Ferramenta de Matriz de interoperabilidade". Uma malha pode consistir em um ou vários switches, e os controladores de storage podem ser conectados a vários switches.

Vários hosts, usando sistemas operacionais diferentes, como Windows, Linux ou UNIX, podem acessar os controladores de storage ao mesmo tempo. Os hosts exigem que uma solução de multipathing suportada seja instalada e configurada. Sistemas operacionais suportados e soluções multipathing podem ser verificados na ferramenta Matriz de interoperabilidade.

Configurações MultiFabric FC e FC-NVMe

Nas configurações de par de HA com várias malhas, há dois ou mais switches que conectam pares de HA a um ou mais hosts. Para simplificar, a figura a seguir de par de HA com várias malhas mostra apenas duas malhas, mas você pode ter duas ou mais malhas em qualquer configuração de várias malhas.

Os números de porta de destino FC (0C, 0d, 1a, 1b) nas ilustrações são exemplos. Os números reais das portas variam dependendo do modelo do nó de armazenamento e se você está usando adaptadores de expansão.

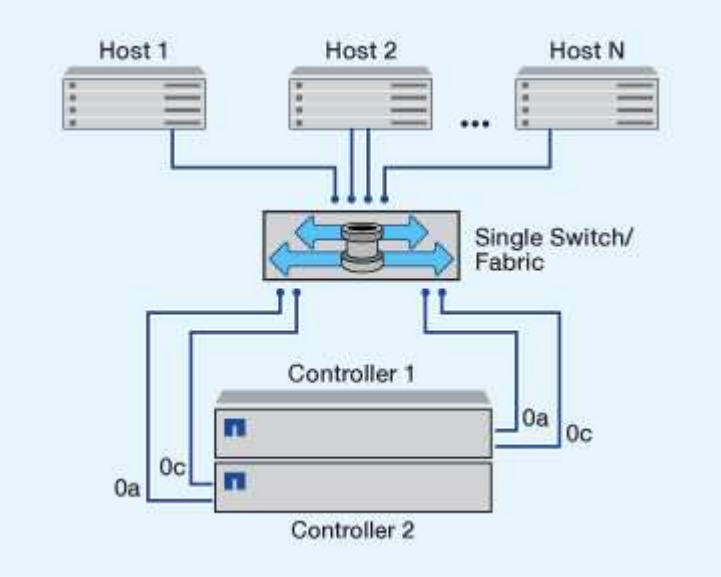


Configurações FC de malha única e FC-NVMe

Nas configurações de par de HA de estrutura única, há uma malha que conecta ambas as controladoras no par de HA a um ou mais hosts. Como os hosts e as controladoras são conectados por meio de um único switch, as configurações de par de HA de estrutura única não são totalmente redundantes.

Os números de porta de destino FC (0a, 0C) nas ilustrações são exemplos. Os números reais das portas variam dependendo do modelo do nó de armazenamento e se você está usando adaptadores de expansão.

Todas as plataformas compatíveis com configurações de FC são compatíveis com configurações de par de HA de malha única.



"Configurações de nó único" não são recomendadas porque não fornecem a redundância necessária para dar suporte à tolerância de falhas e operações ininterruptas.

Informações relacionadas

- Saiba como "Mapeamento LUN seletivo (SLM)" limita os caminhos utilizados para acessar as LUNs de propriedade de um par de HA.
- Saiba mais "SAN LIFs"sobre .

Práticas recomendadas de configuração de switch FC

Para obter o melhor desempenho, você deve considerar certas práticas recomendadas ao configurar seu switch FC.

Uma configuração de velocidade de link fixo é a prática recomendada para configurações de switch FC, especialmente para malhas grandes, porque fornece o melhor desempenho para recompilações de malha e pode economizar tempo de maneira significativa. Embora a negociação automática forneça a maior flexibilidade, a configuração do switch FC nem sempre funciona conforme o esperado e adiciona tempo à sequência geral de construção da malha.

Todos os switches que estão conetados à malha devem suportar a virtualização N_Port ID (NPIV) e devem ter o NPIV habilitado. O ONTAP usa NPIV para apresentar metas FC em uma malha.

Para obter detalhes sobre quais ambientes são suportados, consulte o "Ferramenta de Matriz de

interoperabilidade do NetApp".

Para obter as práticas recomendadas de FC e iSCSI, "Relatório técnico da NetApp 4080: Práticas recomendadas para SAN moderna" consulte .

Número suportado de contagens de saltos FC

A contagem máxima de FC HOP suportada entre um host e um sistema de storage depende do fornecedor do switch e do suporte do sistema de storage para configurações FC.

A contagem de saltos é definida como o número de switches no caminho entre o iniciador (host) e o destino (sistema de armazenamento). Cisco também se refere a esse valor como o *diâmetro da malha SAN*.

Fornecedor do interrutor	Contagem de saltos suportada
Brocade	7 para FC, 5 para FCoE
Cisco	7 para FC, até 3 dos switches podem ser switches FCoE.

Informações relacionadas

"Downloads do NetApp: Documentos da matriz de escalabilidade do Brocade"

"Downloads do NetApp: Documentos da matriz de escalabilidade do Cisco"

Recomendações de configuração de porta de destino FC

As portas de destino FC podem ser configuradas e usadas no protocolo FC-NVMe da mesma maneira que são configuradas e usadas no protocolo FC. O suporte ao protocolo FC-NVMe varia de acordo com a sua plataforma e a versão do ONTAP. Use o NetApp Hardware Universe para verificar o suporte.

Para obter o melhor desempenho e a mais alta disponibilidade, você deve usar a configuração de porta de destino recomendada listada na "NetApp Hardware Universe" para sua plataforma específica.

Configuração para portas de destino FC com ASICs compartilhados

As plataformas a seguir têm pares de portas com circuitos integrados (ASICs) específicos de aplicativos compartilhados. Se você usar um adaptador de expansão com essas plataformas, configure suas portas FC para que elas não usem o mesmo ASIC para conetividade.

Controlador	Pares de portas com ASIC partilhado	Número de portas de destino: Portas recomendadas
• FAS8200 • AFF A300	0g-0h	1: 0g 2: 0g, 0h

Controlador	Pares de portas com ASIC partilhado	Número de portas de destino: Portas recomendadas
• FAS2720 • FAS2750 • AFF A220	0c-0d 0e-0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

Velocidades compatíveis com porta de destino FC

As portas de destino FC podem ser configuradas para serem executadas em diferentes velocidades. Todas as portas de destino usadas por um determinado host devem ser definidas para a mesma velocidade. Você deve definir a velocidade da porta de destino para corresponder à velocidade do dispositivo ao qual ela se coneta. Não use a negociação automática para a velocidade da porta. Uma porta definida como negociação automática pode levar mais tempo para se reconetar após uma tomada de controle/giveback ou outra interrupção.

É possível configurar portas integradas e adaptadores de expansão para serem executados nas seguintes velocidades. Cada porta do controlador e adaptador de expansão pode ser configurada individualmente para diferentes velocidades, conforme necessário.

Portas de 4 GB	Portas de 8 GB	Portas de 16 GB	Portas de 32 GB
• 4 GB • 2 GB • 1 GB	• 8 GB • 4 GB • 2 GB	• 16 GB • 8 GB • 4 GB	• 32 GB • 16 GB • 8 GB

As portas UTA2 podem usar um adaptador SFP de 8 GB para suportar velocidades de 8, 4 e 2 GB, se necessário.

Gerenciar sistemas com adaptadores FC

Visão geral do gerenciamento de sistemas com adaptadores FC

Os comandos estão disponíveis para gerenciar adaptadores FC integrados e placas adaptadoras FC. Esses comandos podem ser usados para configurar o modo do adaptador, exibir informações do adaptador e alterar a velocidade.

A maioria dos sistemas de storage tem adaptadores FC integrados que podem ser configurados como iniciadores ou destinos. Você também pode usar placas de adaptador FC configuradas como iniciadores ou destinos. Os iniciadores se conetam aos compartimentos de disco back-end e, possivelmente, a matrizes de armazenamento estranho (FlexArray). Os destinos se conetam apenas aos switches FC. Ambas as portas HBA de destino FC e a velocidade da porta do switch devem ser definidas para o mesmo valor e não devem ser definidas para auto.

Comandos para gerenciar adaptadores FC

Você pode usar comandos FC para gerenciar adaptadores de destino FC, adaptadores iniciadores FC e adaptadores FC integrados para o controlador de storage. Os mesmos comandos são usados para gerenciar adaptadores FC para o protocolo FC e o protocolo

FC-NVMe.

Os comandos do adaptador do iniciador FC funcionam apenas no nível do nó. Você deve usar o `run -node node_name` comando antes de usar os comandos do adaptador do iniciador FC.

Comandos para gerenciar adaptadores de destino FC

Se você quiser…	Use este comando…
Exibir as informações do adaptador FC em um nó	`network fcp adapter show`
Modifique os parâmetros do adaptador de destino FC	`network fcp adapter modify`
Apresentar informações de tráfego do protocolo FC	`run -node node_name sysstat -f`
Apresentar durante quanto tempo o protocolo FC foi executado	`run -node node_name uptime`
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`
Exibir uma página de manual para um comando	`man command_name`

Comandos para gerenciar adaptadores de iniciador FC

Se você quiser…	Use este comando…
Exibir informações para todos os iniciadores e seus adaptadores em um nó	`run -node node_name storage show adapter`
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`

Comandos para gerenciar adaptadores FC integrados

Se você quiser…	Use este comando…
Exibir o status das portas FC integradas	`system node hardware unified-connect show`

Configurar adaptadores FC para o modo iniciador

Você pode configurar portas FC individuais de adaptadores integrados e determinadas placas de adaptador FC para o modo iniciador. O modo iniciador é usado para conetar as portas a unidades de fita, bibliotecas de fita ou armazenamento de terceiros com virtualização FlexArray ou importação de LUN estrangeiro (FLI).

O que você vai precisar

- Os LIFs no adaptador devem ser removidos de quaisquer conjuntos de portas dos quais sejam membros.
- Todos os LIF de todas as máquinas virtuais de armazenamento (SVM) que usam a porta física a ser modificada devem ser migrados ou destruídos antes de alterar a personalidade da porta física de destino para iniciador.

Sobre esta tarefa

Cada porta FC integrada pode ser configurada individualmente como iniciador ou destino. As portas em certos adaptadores FC também podem ser configuradas individualmente como uma porta de destino ou uma porta de iniciador, assim como as portas FC integradas. Uma lista de adaptadores que podem ser configurados para o modo de destino está disponível no "NetApp Hardware Universe".

O NVMe/FC oferece suporte ao modo iniciador.

Passos

1. Remova todas as LIFs do adaptador:

   `network interface delete -vserver SVM_name -lif lif_name,lif_name`

2. Coloque o adaptador offline:

   `network fcp adapter modify -node node_name -adapter adapter_port -status-admin down`

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

3. Altere o adaptador de destino para iniciador:

   `system hardware unified-connect modify -t initiator adapter_port`

4. Reinicie o nó que hospeda o adaptador que você alterou.
5. Verifique se as portas FC estão configuradas no estado correto para sua configuração:

   `system hardware unified-connect show`

6. Coloque o adaptador novamente online:

   `node run -node node_name storage enable adapter adapter_port`

Configurar adaptadores FC para o modo de destino

Você pode configurar portas FC individuais de adaptadores integrados e determinadas placas de adaptador FC para o modo de destino. O modo de destino é usado para

conetar as portas aos iniciadores FC.

Sobre esta tarefa

Cada porta FC integrada pode ser configurada individualmente como iniciador ou destino. As portas em certos adaptadores FC também podem ser configuradas individualmente como uma porta de destino ou uma porta de iniciador, assim como as portas FC integradas. Uma lista de adaptadores que podem ser configurados para o modo de destino está disponível no "NetApp Hardware Universe".

As mesmas etapas são usadas na configuração de adaptadores FC para o protocolo FC e para o protocolo FC-NVMe. No entanto, apenas certos adaptadores FC são compatíveis com FC-NVMe. Consulte "NetApp Hardware Universe" a para obter uma lista de adaptadores compatíveis com o protocolo FC-NVMe.

Passos

1. Coloque o adaptador offline:

   `node run -node` *`node_name`* `storage disable adapter` *`adapter_name`*

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

2. Altere o adaptador do iniciador para o destino:

   `system node hardware unified-connect modify -t target -node` *`node_name`* `adapter` *`adapter_name`*

3. Reinicie o nó que hospeda o adaptador que você alterou.
4. Verifique se a porta de destino tem a configuração correta:

   `network fcp adapter show -node` *`node_name`*

5. Coloque o adaptador online:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_port`* `-state up`

Exibir informações sobre um adaptador de destino FC

Você pode usar o `network fcp adapter show` comando para exibir as informações de configuração do sistema e do adaptador para qualquer adaptador FC no sistema.

Passo

1. Exiba informações sobre o adaptador FC usando o `network fcp adapter show` comando.

   A saída exibe informações de configuração do sistema e informações do adaptador para cada slot usado.

   `network fcp adapter show -instance -node node1 -adapter 0a`

Altere a velocidade do adaptador FC

Você deve definir a velocidade da porta de destino do adaptador para corresponder à velocidade do dispositivo ao qual ele se coneta, em vez de usar a negociação automática. Uma porta definida como negociação automática pode levar mais tempo

para se reconetar após uma tomada de controle/giveback ou outra interrupção.

O que você vai precisar

Todos os LIFs que usam esse adaptador como porta inicial devem estar offline.

Sobre esta tarefa

Como essa tarefa abrange todas as máquinas virtuais de armazenamento (SVMs) e todas as LIFs em um cluster, você deve usar os `-home-port` parâmetros e `-home-lif` para limitar o escopo dessa operação. Se você não usar esses parâmetros, a operação se aplica a todos os LIFs no cluster, o que pode não ser desejável.

Passos

1. Tire todos os LIFs neste adaptador offline:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin down
   ```

2. Coloque o adaptador offline:

   ```
   network fcp adapter modify -node node1 -adapter 0c -state down
   ```

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

3. Determine a velocidade máxima do adaptador de porta:

   ```
   fcp adapter show -instance
   ```

   Não é possível modificar a velocidade do adaptador para além da velocidade máxima.

4. Alterar a velocidade do adaptador:

   ```
   network fcp adapter modify -node node1 -adapter 0c -speed 16
   ```

5. Coloque o adaptador online:

   ```
   network fcp adapter modify -node node1 -adapter 0c -state up
   ```

6. Coloque todos os LIFs no adaptador online:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin up
   ```

Portas FC compatíveis

O número de portas FC integradas e portas CNA/UTA2 configuradas para FC varia de acordo com o modelo da controladora. As portas FC também estão disponíveis por meio de adaptadores de expansão de destino FC compatíveis ou placas UTA2 adicionais configuradas com adaptadores FC SFP mais.

FC integrado, UTA e portas de UTA2 GbE

- As portas integradas podem ser configuradas individualmente como portas FC de destino ou iniciador.
- O número de portas FC integradas difere dependendo do modelo do controlador.

  O "NetApp Hardware Universe" contém uma lista completa de portas FC integradas em cada modelo de controladora.

- Os sistemas FAS2520 não são compatíveis com FC.

Portas FC do adaptador de expansão de destino

- Os adaptadores de expansão de destino disponíveis diferem dependendo do modelo do controlador.

  O "NetApp Hardware Universe" contém uma lista completa dos adaptadores de expansão de destino para cada modelo de controlador.

- As portas em alguns adaptadores de expansão FC são configuradas como iniciadores ou destinos na fábrica e não podem ser alteradas.

  Outras podem ser configuradas individualmente como portas FC de destino ou iniciador, assim como as portas FC integradas. Uma lista completa está disponível em "NetApp Hardware Universe".

Evite a perda de conetividade ao usar o adaptador X1133A-R6

Você pode evitar a perda de conetividade durante uma falha de porta configurando o sistema com caminhos redundantes para separar HBAs X1133A-R6.

O HBA X1133A-R6 é um adaptador FC de 4 portas e 16 GB que consiste em dois pares de 2 portas. O adaptador X1133A-R6 pode ser configurado como modo de destino ou modo de iniciador. Cada par de 2 portas é suportado por um único ASIC (por exemplo, porta 1 e porta 2 no ASIC 1 e porta 3 e porta 4 no ASIC 2). Ambas as portas em um único ASIC devem ser configuradas para operar no mesmo modo, seja no modo de destino ou no modo de iniciador. Se ocorrer um erro com o ASIC que suporta um par, ambas as portas do par ficam offline.

Para evitar essa perda de conetividade, configure o sistema com caminhos redundantes para separar HBAs X1133A-R6 ou com caminhos redundantes para portas compatíveis com ASICs diferentes no HBA.

Configurações FCoE

Maneiras de configurar a visão geral do FCoE

O FCoE pode ser configurado de várias maneiras usando switches FCoE. Configurações com conexão direta não são compatíveis com FCoE.

Todas as configurações FCoE são de estrutura dupla, totalmente redundantes e exigem software de multipathing no lado do host. Em todas as configurações FCoE, você pode ter vários switches FCoE e FC no caminho entre o iniciador e o destino, até o limite máximo de contagem de saltos. Para conetar switches entre si, os switches devem executar uma versão de firmware que suporte ISLs Ethernet. Cada host em qualquer configuração FCoE pode ser configurado com um sistema operacional diferente.

As configurações FCoE exigem switches Ethernet que suportam explicitamente os recursos FCoE. As configurações FCoE são validadas pelo mesmo processo de interoperabilidade e garantia de qualidade que

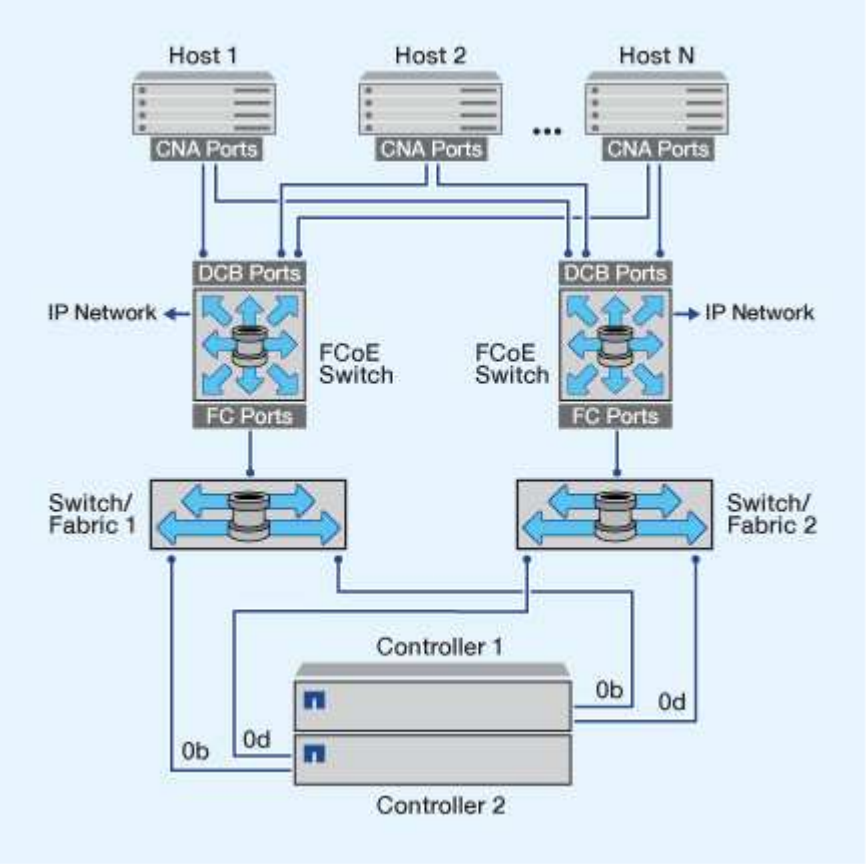
os switches FC. As configurações suportadas estão listadas na Matriz de interoperabilidade. Alguns dos parâmetros incluídos nessas configurações suportadas são o modelo de switch, o número de switches que podem ser implantados em uma única malha e a versão de firmware de switch suportada.

Os números da porta do adaptador de expansão de destino FC nas ilustrações são exemplos. Os números reais das portas podem variar, dependendo dos slots de expansão nos quais os adaptadores de expansão de destino FCoE estão instalados.

Iniciador FCoE para destino FC

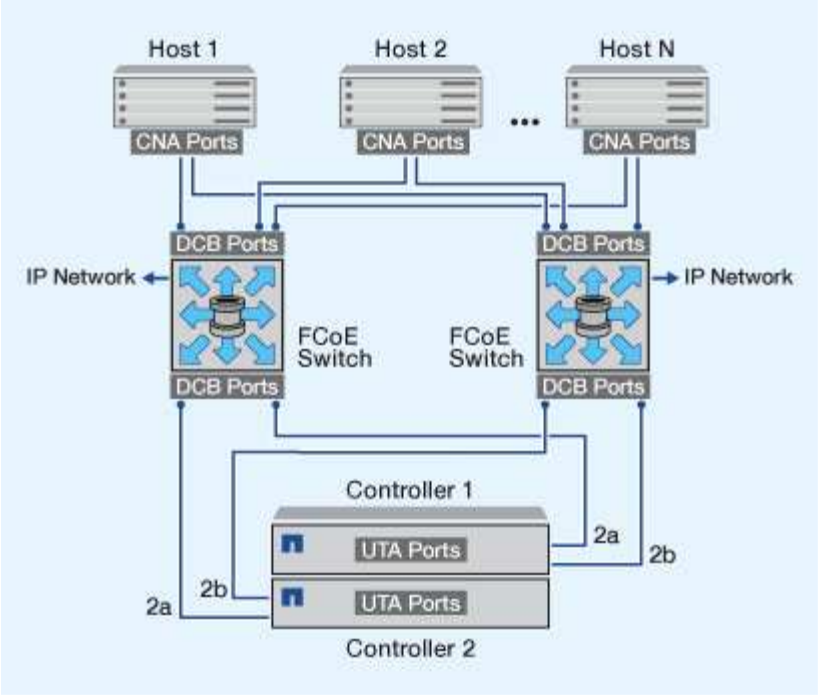
Usando os iniciadores FCoE (CNAs), você pode conetar hosts a ambos os controladores em um par de HA por meio de switches FCoE a portas de destino FC. O switch FCoE também deve ter portas FC. O iniciador FCoE do host sempre se coneta ao switch FCoE. O switch FCoE pode se conectar diretamente ao destino FC ou pode se conectar ao destino FC por meio de switches FC.

A ilustração a seguir mostra CNAs do host conetando-se a um switch FCoE e, em seguida, a um switch FC antes de se conetar ao par de HA:



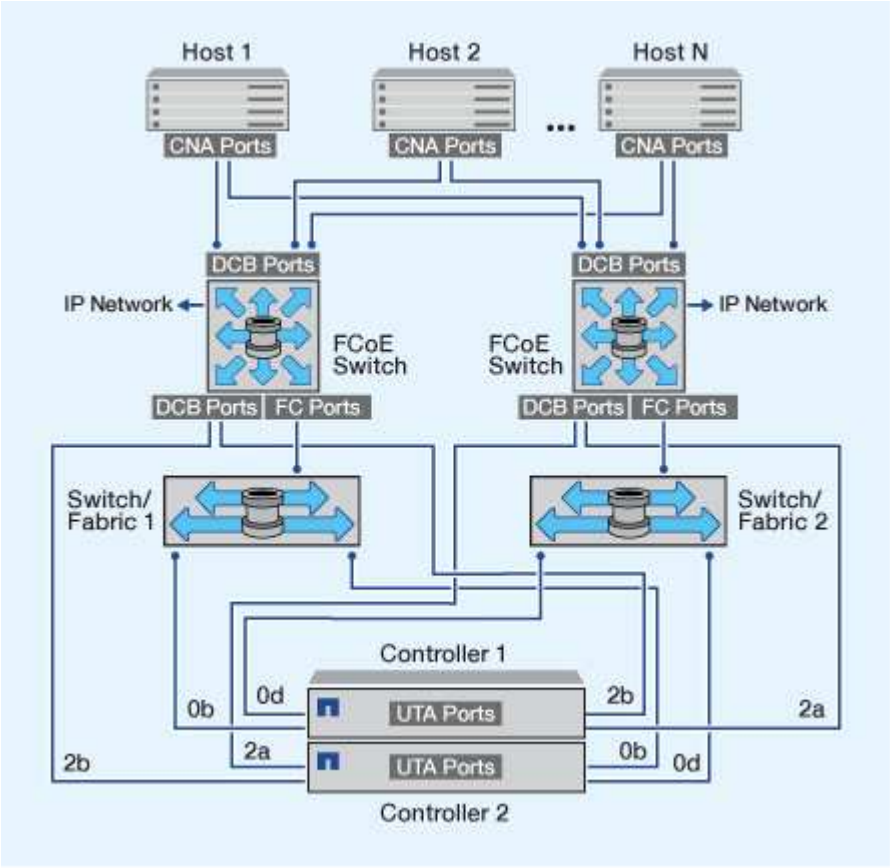
Iniciador FCoE para destino FCoE

Usando os iniciadores FCoE de host (CNAs), você pode conetar hosts a ambos os controladores em um par de HA a portas de destino FCoE (também chamadas de UTA ou UTA2s) por meio de switches FCoE.



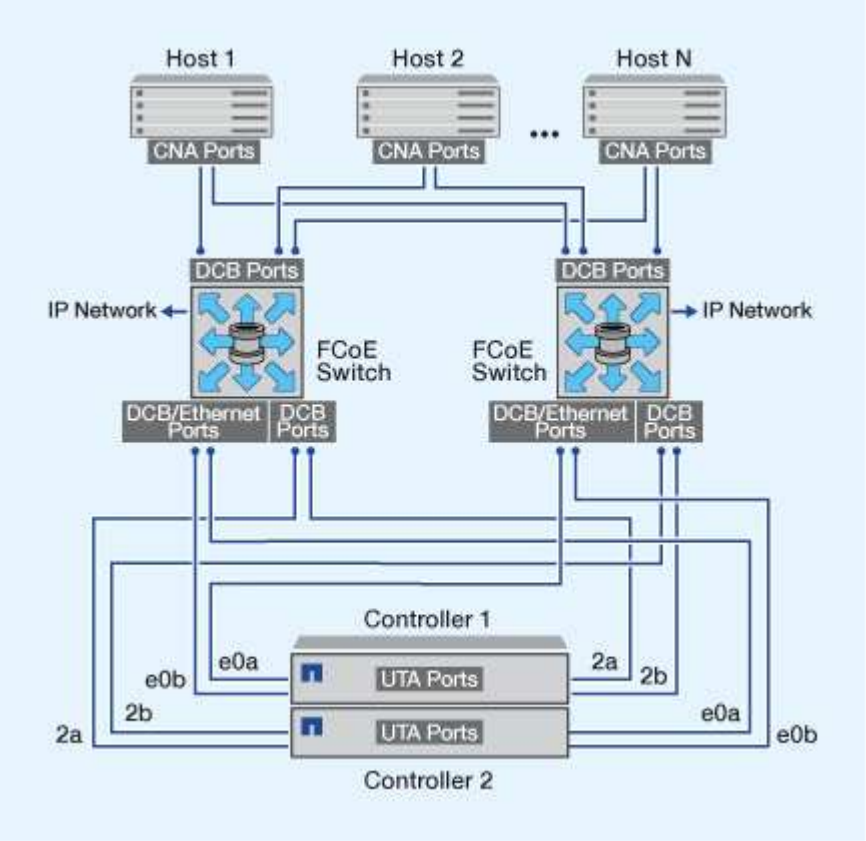
Iniciador FCoE para destinos FCoE e FC

Usando os iniciadores FCoE de host (CNAs), você pode conetar hosts a ambos os controladores em um par de HA a portas de destino FCoE e FC (também chamadas de UTA ou UTA2s) por meio de switches FCoE.



FCoE misturado com protocolos de storage IP

Usando os iniciadores FCoE de host (CNAs), você pode conetar hosts a ambos os controladores em um par de HA a portas de destino FCoE (também chamadas de UTA ou UTA2s) por meio de switches FCoE. As portas FCoE não podem usar a agregação de links tradicional a um único switch. Os switches Cisco suportam um tipo especial de agregação de links (Canal de porta virtual) que suporta FCoE. Um canal de porta virtual agrega links individuais a dois switches. Você também pode usar canais de porta virtual para outro tráfego Ethernet. As portas usadas para tráfego diferente do FCoE, incluindo NFS, SMB, iSCSI e outro tráfego Ethernet, podem usar portas Ethernet regulares nos switches FCoE.



Combinações de iniciador FCoE e destino

Certas combinações de iniciadores e destinos FC tradicionais e FCoE são suportadas.

Iniciadores FCoE

Você pode usar iniciadores FCoE em computadores host com destinos FCoE e FC tradicionais em controladores de armazenamento. O iniciador FCoE do host deve se conetar a um switch FCoE DCB (ponte de data center); a conexão direta a um destino não é suportada.

A tabela a seguir lista as combinações suportadas:

Iniciador	Alvo	Suportado?
FC	FC	Sim
FC	FCoE	Sim

Iniciador	Alvo	Suportado?
FCoE	FC	Sim
FCoE	FCoE	Sim

Destinos FCoE

É possível misturar portas de destino FCoE com portas FC de 4 GB, 8 GB ou 16 GB na controladora de storage, independentemente de as portas FC serem adaptadores de destino complementares ou portas integradas. Você pode ter adaptadores de destino FCoE e FC no mesmo controlador de storage.

As regras da combinação de portas FC integradas e de expansão ainda se aplicam.

Contagem de saltos com suporte para FCoE

A contagem máxima de saltos Fibre Channel over Ethernet (FCoE) suportada entre um host e um sistema de armazenamento depende do fornecedor do switch e do suporte do sistema de armazenamento para configurações FCoE.

A contagem de saltos é definida como o número de switches no caminho entre o iniciador (host) e o destino (sistema de armazenamento). A documentação da Cisco Systems também se refere a esse valor como o *diâmetro da malha SAN*.

Para FCoE, você pode ter switches FCoE conetados a switches FC.

Para conexões FCoE de ponta a ponta, os switches FCoE devem estar executando uma versão de firmware que suporte ISLs (links inter-switch Ethernet).

A tabela a seguir lista o máximo de contagens de saltos suportadas:

Fornecedor do interrutor	Contagem de saltos suportada
Brocade	7 para FC 5 para FCoE
Cisco	7 Até 3 dos switches podem ser switches FCoE.

Zoneamento Fibre Channel e FCoE

Visão geral do zoneamento Fibre Channel e FCoE

Uma zona FC, FC-NVMe ou FCoE é um agrupamento lógico de uma ou mais portas em uma malha. Para que os dispositivos possam se ver, conetar, criar sessões entre si e se comunicar, ambas as portas precisam ter uma associação de zona comum. Recomenda-se um zoneamento de iniciador único.

Razões para o zoneamento

- O zoneamento reduz ou elimina *crosstalk* entre HBAs iniciador.

  Isso ocorre mesmo em ambientes pequenos e é um dos melhores argumentos para a implementação do zoneamento. Os subconjuntos de tecido lógico criados pelo zoneamento eliminam problemas de conversa cruzada.

- O zoneamento reduz o número de caminhos disponíveis para uma porta FC, FC-NVMe ou FCoE específica e reduz o número de caminhos entre um host e um LUN específico visível.

  Por exemplo, algumas soluções de multipathing do sistema operacional host têm um limite no número de caminhos que podem gerenciar. O zoneamento pode reduzir o número de caminhos que um driver de multipathing do sistema operacional vê. Se um host não tiver uma solução multipathing instalada, você precisará verificar se apenas um caminho para um LUN é visível usando o zoneamento na malha ou uma combinação de mapeamento de LUN seletivo (SLM) e portsets no SVM.

- O zoneamento aumenta a segurança limitando o acesso e a conetividade a pontos finais que compartilham uma zona comum.

  Portas que não têm zonas em comum não podem se comunicar umas com as outras.

- O zoneamento melhora a confiabilidade da SAN isolando problemas que ocorrem e ajuda a reduzir o tempo de resolução de problemas limitando o espaço do problema.

Recomendações para zoneamento

- Você deve implementar o zoneamento a qualquer momento, se quatro ou mais hosts estiverem conetados a uma SAN ou se o SLM não for implementado nos nós a uma SAN.
- Embora o World Wide Node Name zoning seja possível com alguns fornecedores de switch, o World Wide Port Name zoning é necessário para definir adequadamente uma porta específica e usar o NPIV de forma eficaz.
- Você deve limitar o tamanho da zona, mantendo a capacidade de gerenciamento.

  Várias zonas podem se sobrepor ao tamanho limite. Idealmente, uma zona é definida para cada host ou cluster de host.

- Você deve usar o zoneamento de um único iniciador para eliminar a interferência cruzada entre HBAs do iniciador.

Zoneamento baseado em nome mundial

O zoneamento baseado no World Wide Name (WWN) especifica o WWN dos membros a serem incluídos na zona. Ao zonear no ONTAP, você deve usar o zoneamento de nome de porta mundial (WWPN).

WWPN zoneamento fornece flexibilidade porque o acesso não é determinado por onde o dispositivo está fisicamente conetado à malha. Você pode mover um cabo de uma porta para outra sem reconfigurar zonas.

Para caminhos Fibre Channel para controladores de storage que executam ONTAP, verifique se os switches FC estão zoneados usando WWPNs das interfaces lógicas de destino (LIFs), e não as WWPNs das portas físicas no nó. Para obter mais informações sobre LIFs, consulte o *Guia de Gerenciamento de rede do ONTAP*.

"Gerenciamento de rede"

Zonas individuais

Na configuração de zoneamento recomendada, há um iniciador de host por zona. A zona consiste na porta do iniciador do host e em um ou mais LIFs de destino nos nós de storage que estão fornecendo acesso aos LUNs até o número desejado de caminhos por destino. Isso significa que os hosts que acessam os mesmos nós não podem ver as portas uns dos outros, mas cada iniciador pode acessar qualquer nó.

Você deve adicionar todos os LIF da máquina virtual de armazenamento (SVM) na zona com o iniciador do host. Isso permite que você mova volumes ou LUNs sem editar suas zonas existentes ou criar novas zonas.

Para caminhos de Fibre Channel para nós que executam ONTAP, certifique-se de que os switches FC sejam zoneados usando WWPNs das interfaces lógicas de destino (LIFs), e não as WWPNs das portas físicas no nó. As WWPNs dos portos físicos começam com "50" e as WWPNs dos LIFs começam com ""20"".

Zoneamento de tecido único

Em uma configuração de estrutura única, você ainda pode conectar cada iniciador de host a cada nó de storage. O software multipathing é necessário no host para gerenciar vários caminhos. Cada host deve ter dois iniciadores para multipathing para fornecer resiliência na solução.

Cada iniciador deve ter um mínimo de um LIF de cada nó que o iniciador possa acessar. O zoneamento deve permitir pelo menos um caminho do iniciador do host para o par de nós de HA no cluster para fornecer um caminho para a conetividade LUN. Isso significa que cada iniciador no host pode ter apenas um LIF de destino por nó em sua configuração de zona. Se houver um requisito de multipathing para o mesmo nó ou vários nós no cluster, cada nó terá várias LIFs por nó em sua configuração de zona. Isso permite que o host ainda acesse seus LUNs se um nó falhar ou se um volume contendo o LUN for movido para um nó diferente. Isso também requer que os nós de relatório sejam definidos adequadamente.

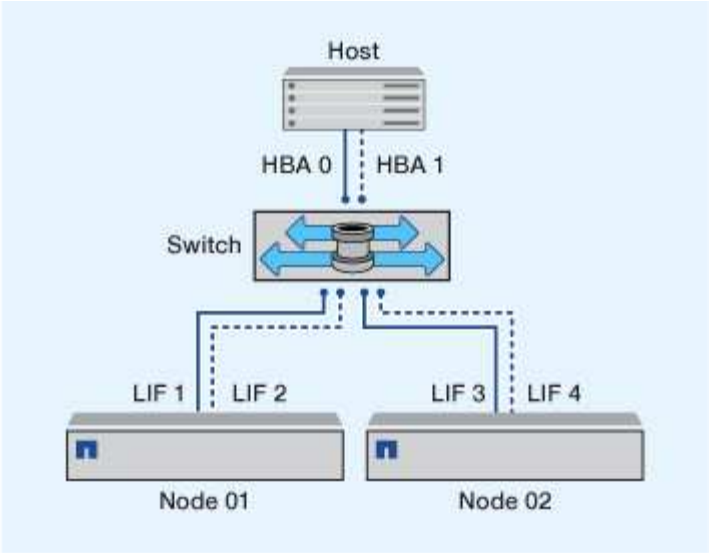
Configurações de estrutura única são compatíveis, mas não são consideradas altamente disponíveis. A falha de um único componente pode causar perda de acesso aos dados.

Na figura a seguir, o host tem dois iniciadores e está executando software multipathing. Existem duas zonas:

> A convenção de nomenclatura usada nesta figura é apenas uma recomendação de uma possível convenção de nomenclatura que você pode escolher usar para sua solução ONTAP.

- Zona 1: HBA 0, LIF_1 e LIF_3
- Zona 2: HBA 1, LIF_2 e LIF_4

Se a configuração incluísse mais nós, as LIFs para os nós adicionais seriam incluídas nessas zonas.



Neste exemplo, você também pode ter todos os quatro LIFs em cada zona. Nesse caso, as zonas seriam as seguintes:

- Zona 1: HBA 0, LIF_1, LIF_2, LIF_3 e LIF_4
- Zona 2: HBA 1, LIF_1, LIF_2, LIF_3 e LIF_4

O sistema operacional host e o software de multipathing precisam dar suporte ao número de caminhos compatíveis que estão sendo usados para acessar os LUNs nos nós. Para determinar o número de caminhos usados para acessar os LUNs nos nós, consulte a seção limites de configuração da SAN.

Informações relacionadas

"NetApp Hardware Universe"

Zoneamento de par HA de estrutura dupla

Em configurações de estrutura dupla, é possível conectar cada iniciador de host a cada nó de cluster. Cada iniciador de host usa um switch diferente para acessar os nós de cluster. O software multipathing é necessário no host para gerenciar vários caminhos.

Configurações de estrutura dupla são consideradas de alta disponibilidade porque o acesso aos dados é mantido em caso de falha em um único componente.

Na figura a seguir, o host tem dois iniciadores e está executando software multipathing. Existem duas zonas. O SLM é configurado para que todos os nós sejam considerados como nós de relatório.

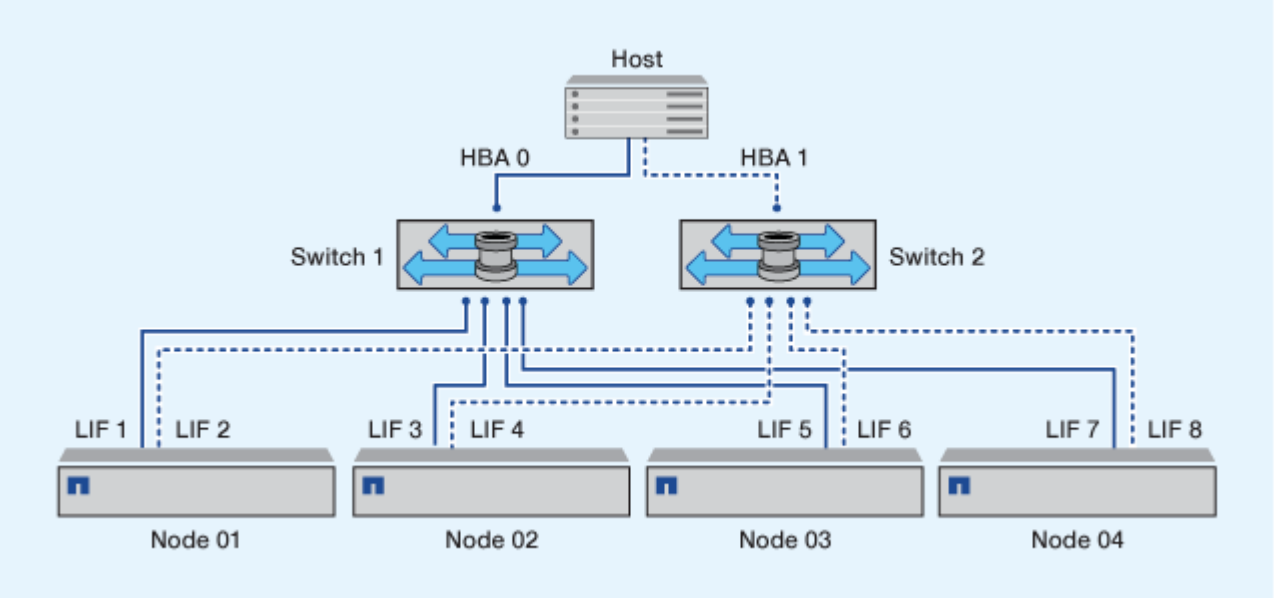
A convenção de nomenclatura usada nesta figura é apenas uma recomendação de uma possível convenção de nomenclatura que você pode escolher usar para sua solução ONTAP.

- Zona 1: HBA 0, LIF_1, LIF_3, LIF_5 e LIF_7
- Zona 2: HBA 1, LIF_2, LIF_4, LIF_6 e LIF_8

Cada iniciador do host é zoneado por um switch diferente. A zona 1 é acessada através do interrutor 1. A zona 2 é acessada através do interrutor 2.

Cada iniciador pode acessar um LIF em cada nó. Isso permite que o host ainda acesse LUNs se um nó falhar. Os SVMs têm acesso a todas as LIFs iSCSI e FC em cada nó em uma solução em cluster com base na configuração de mapa LUN seletivo (SLM) e na configuração do nó de relatório. Você pode usar o zoneamento de switch SLM, portsets ou FC para reduzir o número de caminhos de uma SVM para o host e o número de caminhos de uma SVM para um LUN.

Se a configuração incluísse mais nós, as LIFs para os nós adicionais seriam incluídas nessas zonas.



O sistema operacional host e o software multipathing precisam dar suporte ao número de caminhos que estão sendo usados para acessar os LUNs nos nós.

Informações relacionadas

"NetApp Hardware Universe"

Restrições de zoneamento para switches Cisco FC e FCoE

Ao usar os switches FC e FCoE Cisco, uma única zona de malha não deve conter mais de um LIF de destino para a mesma porta física. Se várias LIFs na mesma porta estiverem na mesma zona, as portas LIF podem falhar ao recuperar de uma perda de conexão.

Os switches FC comuns são usados no protocolo FC-NVMe da mesma maneira que são usados no protocolo FC.

- Várias LIFs para os protocolos FC e FCoE podem compartilhar portas físicas em um nó, contanto que estejam em zonas diferentes.
- O FC-NVMe e o FCoE não podem compartilhar a mesma porta física.
- FC e FC-NVMe podem compartilhar a mesma porta física de 32 GB.
- Os switches FC e FCoE da Cisco exigem que cada LIF em uma determinada porta esteja em uma zona separada das outras LIFs nessa porta.
- Uma única zona pode ter LIFs FC e FCoE. Uma zona pode conter um LIF de cada porta de destino no cluster, mas tenha cuidado para não exceder os limites de caminho do host e verificar a configuração do SLM.

- LIFs em diferentes portas físicas podem estar na mesma zona.
- Os switches Cisco exigem que os LIFs sejam separados.

  Embora não seja necessário, recomenda-se separar LIFs para todos os switches

Requisitos para configurações de SAN compartilhadas

Configurações de SAN compartilhadas são definidas como hosts conectados aos sistemas de storage da ONTAP e aos sistemas de storage de outros fornecedores. O acesso aos sistemas de storage da ONTAP e aos sistemas de storage de outros fornecedores a partir de um único host é suportado, desde que sejam atendidos vários requisitos.

Para todos os sistemas operacionais host, é uma prática recomendada usar adaptadores separados para se conetar aos sistemas de storage de cada fornecedor. O uso de adaptadores separados reduz as chances de drivers e configurações conflitantes. Para conexões com um sistema de armazenamento ONTAP, o modelo do adaptador, BIOS, firmware e driver devem ser listados como suportados na ferramenta de Matriz de interoperabilidade do NetApp.

Você deve definir os valores de tempo limite necessários ou recomendados e outros parâmetros de armazenamento para o host. Você deve sempre instalar o software NetApp ou aplicar as configurações do NetApp por último.

- Para o AIX, você deve aplicar os valores da versão do AIX Host Utilities listada na ferramenta de Matriz de interoperabilidade para sua configuração.
- Para o ESX, você deve aplicar as configurações do host usando o Virtual Storage Console para VMware vSphere.
- Para HP-UX, você deve usar as configurações de armazenamento padrão HP-UX.
- Para Linux, você deve aplicar os valores da versão Linux Host Utilities listada na ferramenta de Matriz de interoperabilidade para sua configuração.
- Para o Solaris, você deve aplicar os valores da versão do Solaris Host Utilities listada na ferramenta de Matriz de interoperabilidade para sua configuração.
- Para o Windows, você deve instalar a versão do Windows Host Utilities que está listada na ferramenta de Matriz de interoperabilidade para sua configuração.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Configurações DE SAN em um ambiente MetroCluster

Configurações DE SAN em um ambiente MetroCluster

Você precisa estar ciente de algumas considerações ao usar configurações de SAN em um ambiente MetroCluster.

- As configurações do MetroCluster não são compatíveis com configurações VSAN "roteadas" de malha FC de front-end.
- A partir do ONTAP 9.15,1, as configurações de IP MetroCluster de quatro nós são compatíveis com NVMe/TCP.

- A partir do ONTAP 9.12,1, as configurações de IP MetroCluster de quatro nós são compatíveis com NVMe/FC. As configurações do MetroCluster não são compatíveis com redes NVMe front-end anteriores ao ONTAP 9.12,1.
- Outros protocolos SAN, como iSCSI, FC e FCoE, são compatíveis com configurações do MetroCluster.
- Ao usar configurações de cliente SAN, você deve verificar se quaisquer considerações especiais para configurações do MetroCluster estão incluídas nas notas fornecidas no "Ferramenta de Matriz de interoperabilidade do NetApp" (IMT).
- Os sistemas operacionais e os aplicativos devem fornecer resiliência de e/S de 120 segundos para dar suporte ao switchover não planejado automático da MetroCluster e ao switchover tiebreaker ou iniciado por Mediator.
- As configurações do MetroCluster usam as mesmas WWNNs e WWPNs em ambos os lados da malha FC de front-end.

Informações relacionadas

- "Compreender a proteção de dados e a recuperação de desastres da MetroCluster"
- "artigo da Knowledge base: Quais são as considerações de suporte ao host AIX em uma configuração do MetroCluster?"
- "artigo da base de conhecimento: Considerações de suporte a hosts Solaris em uma configuração do MetroCluster"

Evite a sobreposição de portas entre switchover e switchback

Em um ambiente SAN, você pode configurar os switches front-end para evitar sobreposição quando a porta antiga fica off-line e a nova porta entra on-line.

Durante o switchover, a porta FC no local sobrevivente pode fazer login na malha antes que a malha detete que a porta FC no local de desastre está off-line e removeu essa porta dos serviços de nome e diretório.

Se a porta FC no desastre ainda não for removida, a tentativa de login da malha da porta FC no local sobrevivente pode ser rejeitada devido a uma WWPN duplicada. Esse comportamento dos switches FC pode ser alterado para honrar o login do dispositivo anterior e não o existente. Você deve verificar os efeitos desse comportamento em outros dispositivos de malha. Entre em Contato com o fornecedor do switch para obter mais informações.

Escolha o procedimento correto de acordo com o seu tipo de interrutor.

Exemplo 19. Passos

Interrutor Cisco

1. Ligue ao interrutor e inicie sessão.
2. Entre no modo de configuração:

```
switch# config t
switch(config)#
```

3. Substituir a primeira entrada de dispositivo na base de dados do servidor de nomes pelo novo dispositivo:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Nos switches que estão executando o NX-os 8.x, confirme se o tempo limite do flogi quiesce está definido como zero:

   a. Apresentar o timererval quiesce:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Se a saída na etapa anterior não indicar que o timerval é zero, defina-o como zero:

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Interrutor Brocade

1. Ligue ao interrutor e inicie sessão.
2. Introduza o `switchDisable` comando.
3. Digite o `configure` comando e pressione `y` no prompt.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Escolha a definição 1:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Responda aos prompts restantes, ou pressione **Ctrl D**.
6. Introduza o `switchEnable` comando.

Informações relacionadas

"Realização de comutação para testes ou manutenção"

Suporte de host para multipathing

Suporte de host para visão geral de multipathing

O ONTAP sempre usa o Acesso lógico de Unidade assimétrica (ALUA) para caminhos FC e iSCSI. Use configurações de host compatíveis com ALUA para protocolos FC e iSCSI.

A partir do par de HA multipath ONTAP 9.5, o failover/giveback é compatível com configurações NVMe usando o acesso de namespace assíncrono (ANA). No ONTAP 9.4, o NVMe só oferece suporte a um caminho do host para o destino. O host de aplicações precisa gerenciar o failover de caminho para seu parceiro de alta disponibilidade (HA).

Para obter informações sobre quais configurações de host específicas suportam ALUA ou ANA, consulte "Ferramenta de Matriz de interoperabilidade do NetApp" e "Configuração do host SAN ONTAP" para o sistema operacional do seu host.

Quando o software de multipathing do host é necessário

Se houver mais de um caminho das interfaces lógicas (LIFs) da máquina virtual de storage (SVM) para a malha, é necessário software de multipathing. O software multipathing é necessário no host sempre que o host puder acessar um LUN por mais de um caminho.

O software multipathing apresenta um único disco para o sistema operacional para todos os caminhos para um LUN. Sem software multipathing, o sistema operacional poderia tratar cada caminho como um disco separado, o que pode levar à corrupção de dados.

Sua solução é considerada como tendo vários caminhos se você tiver qualquer um dos seguintes:

- Uma única porta de iniciador no host que é anexada a várias LIFs SAN no SVM
- Várias portas de iniciador anexando a um único LIF de SAN no SVM
- Várias portas de iniciador anexadas a várias LIFs SAN no SVM

O software multipathing é recomendado em configurações de HA. Além do mapa LUN seletivo, é recomendável usar o zoneamento de switch FC ou portsets para limitar os caminhos usados para acessar LUNs.

O software multipathing também é conhecido como software MPIO (multipath I/o).

Número recomendado de caminhos do host para nós no cluster

Você não deve exceder mais de oito caminhos do host para cada nó do cluster, prestando atenção ao número total de caminhos que podem ser suportados pelo sistema

operacional do host e pelo multipathing usado no host.

Você deve ter no mínimo dois caminhos por LUN conetando-se a cada nó de relatório por meio do mapa de LUN seletivo (SLM) usado pela máquina virtual de storage (SVM) no cluster. Isso elimina pontos únicos de falha e permite que o sistema sobreviva a falhas de componentes.

Se você tiver quatro ou mais nós no cluster ou mais de quatro portas de destino sendo usadas pelas SVMs em qualquer um de seus nós, use os métodos a seguir para limitar o número de caminhos que podem ser usados para acessar LUNs em seus nós, de modo que você não exceda o máximo recomendado de oito caminhos.

- SLM

  O SLM reduz o número de caminhos do host para o LUN para apenas caminhos no nó proprietário do LUN e do parceiro de HA do nó proprietário. O SLM está ativado por predefinição.

- Portsets para iSCSI
- Mapeamentos do grupo FC de seu host
- Zoneamento do switch FC

Informações relacionadas

"Administração da SAN"

Limites de configuração

Determine o número de nós suportados para configurações SAN

O número de nós por cluster com suporte do ONTAP varia de acordo com a versão do ONTAP, os modelos de controlador de storage no cluster e o protocolo dos nós do cluster.

Sobre esta tarefa

Se qualquer nó no cluster estiver configurado para FC, FC-NVMe, FCoE ou iSCSI, esse cluster estará limitado aos limites de nó SAN. Os limites de nó baseados nos controladores do cluster são listados em *Hardware Universe*.

Passos

1. Vá para "NetApp Hardware Universe".
2. Clique em **plataformas** no canto superior esquerdo (ao lado do botão **Home**) e selecione o tipo de plataforma.
3. Marque a caixa de seleção ao lado de sua versão do ONTAP.

   Uma nova coluna é exibida para você escolher suas plataformas.

4. Marque as caixas de seleção ao lado das plataformas usadas em sua solução.
5. Desmarque a caixa de seleção **Selecionar tudo** na coluna **escolha suas especificações**.
6. Marque a caixa de seleção **máximo de nós por cluster (nas/SAN)**.
7. Clique em **Mostrar resultados**.

Informações relacionadas

"NetApp Hardware Universe"

Determine o número de hosts com suporte por cluster nas configurações FC e FC-NVMe

O número máximo de hosts SAN que podem ser conetados a um cluster varia muito com base em sua combinação específica de vários atributos de cluster, como o número de hosts conetados a cada nó de cluster, iniciadores por host, sessões por host e nós no cluster.

Sobre esta tarefa

Para configurações FC e FC-NVMe, use o número de nexos de iniciador-destino (ITNs) no sistema para determinar se é possível adicionar mais hosts ao cluster.

Uma ITN representa um caminho desde o iniciador do host até o destino do sistema de armazenamento. O número máximo de ITNs por nó nas configurações FC e FC-NVMe é de 2.048. Contanto que você esteja abaixo do número máximo de ITNs, você pode continuar adicionando hosts ao cluster.

Para determinar o número de ITNs usados no cluster, execute as etapas a seguir para cada nó no cluster.

Passos

1. Identifique todas as LIFs em um determinado nó.
2. Execute o seguinte comando para cada LIF no nó:

   ```
   fcp initiator show -fields wwpn, lif
   ```

   O número de entradas exibidas na parte inferior da saída do comando representa o número de ITNs para esse LIF.

3. Registre o número de ITNs exibidos para cada LIF.
4. Adicione o número de ITNs para cada LIF em cada nó do cluster.

   Esse total representa o número de ITNs em seu cluster.

Determine o número suportado de hosts em configurações iSCSI

O número máximo de hosts SAN que podem ser conetados em configurações iSCSI varia muito com base em sua combinação específica de vários atributos de cluster, como o número de hosts conetados a cada nó de cluster, iniciadores por host, logins por host e nós no cluster.

Sobre esta tarefa

O número de hosts que podem ser conetados diretamente a um nó ou que podem ser conetados por meio de um ou mais switches depende do número de portas Ethernet disponíveis. O número de portas Ethernet disponíveis é determinado pelo modelo do controlador e pelo número e tipo de adaptadores instalados no controlador. O número de portas Ethernet suportadas para controladores e adaptadores está disponível em *Hardware Universe*.

Para todas as configurações de cluster de vários nós, você deve determinar o número de sessões iSCSI por nó para saber se você pode adicionar mais hosts ao cluster. Desde que o cluster esteja abaixo do número máximo de sessões iSCSI por nó, você pode continuar a adicionar hosts ao cluster. O número máximo de sessões iSCSI por nó varia de acordo com os tipos de controladores no cluster.

Passos

1. Identifique todos os grupos de portal de destino no nó.
2. Verifique o número de sessões iSCSI para cada grupo de portal de destino no nó:

   `iscsi session show -tpgroup` *`tpgroup`*

   O número de entradas exibidas na parte inferior da saída do comando representa o número de sessões iSCSI para esse grupo de portal de destino.

3. Registe o número de sessões iSCSI apresentadas para cada grupo de portal de destino.
4. Adicione o número de sessões iSCSI para cada grupo de portal de destino no nó.

   O total representa o número de sessões iSCSI no nó.

Limites de configuração do switch FC

Os switches Fibre Channel têm limites máximos de configuração, incluindo o número de logins suportados por porta, grupo de portas, blade e switch. Os fornecedores de switch documentam seus limites suportados.

Cada interface lógica FC (LIF) faz logon em uma porta de switch FC. O número total de logins de um único destino no nó é igual ao número de LIFs mais um login para a porta física subjacente. Não exceda os limites de configuração do fornecedor do switch para logins ou outros valores de configuração. Isso também é válido para os iniciadores que estão sendo usados no lado do host em ambientes virtualizados com NPIV habilitado. Não exceda os limites de configuração do fornecedor do switch para logins para o destino ou os iniciadores que estão sendo usados na solução.

Limites do interrutor Brocade

Você pode encontrar os limites de configuração para switches Brocade nas *Diretrizes de escalabilidade Brocade*.

Limites do switch dos sistemas Cisco

Você pode encontrar os limites de configuração para switches Cisco "Limites de configuração do Cisco" no guia para sua versão do software de switch Cisco.

Calcular a visão geral da profundidade da fila

Talvez seja necessário ajustar a profundidade da fila FC no host para alcançar os valores máximos de ITNs por nó e ventilador de porta FC. O número máximo de LUNs e o número de HBAs que podem se conetar a uma porta FC são limitados pela profundidade de fila disponível nas portas de destino FC.

Sobre esta tarefa

A profundidade da fila é o número de solicitações de e/S (comandos SCSI) que podem ser enfileiradas em uma controladora de armazenamento. Cada solicitação de e/S do HBA iniciador do host para o adaptador de destino do controlador de armazenamento consome uma entrada de fila. Normalmente, uma maior profundidade de fila equivale a um melhor desempenho. No entanto, se a profundidade máxima da fila do controlador de armazenamento for atingida, esse controlador de armazenamento rejeita os comandos de entrada retornando uma resposta QFULL a eles. Se um grande número de hosts estiver acessando um

controlador de armazenamento, você deve Planejar cuidadosamente para evitar condições QFULL, que degradam significativamente o desempenho do sistema e podem levar a erros em alguns sistemas.

Em uma configuração com vários iniciadores (hosts), todos os hosts devem ter profundidades de fila semelhantes. Devido à desigualdade na profundidade da fila entre os hosts conetados ao controlador de armazenamento através da mesma porta de destino, os hosts com menores profundidades de fila estão sendo privados de acesso a recursos por hosts com maiores profundidades de fila.

As seguintes recomendações gerais podem ser feitas sobre as profundidades da fila "sintonização":

- Para sistemas de tamanho pequeno a médio, utilize uma profundidade de fila HBA de 32 mm.
- Para sistemas grandes, utilize uma profundidade de fila HBA de 128 mm.
- Para casos de exceção ou teste de desempenho, use uma profundidade de fila de 256 mm para evitar possíveis problemas de enfileiramento.
- Todos os hosts devem ter as profundidades da fila definidas para valores semelhantes para dar acesso igual a todos os hosts.
- Para evitar penalidades ou erros de desempenho, a profundidade da fila da porta FC de destino do controlador de storage não deve ser excedida.

Passos

1. Conte o número total de iniciadores FC em todos os hosts que se conetam a uma porta de destino FC.
2. Multiplique por 128.
   - Se o resultado for inferior a 2.048, defina a profundidade da fila para todos os iniciadores como 128. Você tem 15 hosts com um iniciador conetado a cada uma das duas portas de destino no controlador de storage. 15 x 128: 1.920. Como 1.920 é menor do que o limite total de profundidade de fila de 2.048, você pode definir a profundidade de fila para todos os iniciadores como 128.
   - Se o resultado for superior a 2.048, avance para o passo 3. Você tem 30 hosts com um iniciador conetado a cada uma das duas portas de destino no controlador de storage. 30 x 128: 3.840. Como o 3.840 é maior do que o limite total de profundidade de fila de 2.048, você deve escolher uma das opções na etapa 3 para correção.
3. Escolha uma das opções a seguir para adicionar mais hosts ao controlador de storage.
   - Opção 1:
     i. Adicione mais portas de destino FC.
     ii. Redistribua seus iniciadores FC.
     iii. Repita os passos 1 e 2. A profundidade de fila desejada de 3.840 mm excede a profundidade de fila disponível por porta. Para remediar isso, você pode adicionar um adaptador de destino FC de duas portas a cada controlador e, em seguida, rezonear seus switches FC para que 15 dos seus hosts 30 se conetem a um conjunto de portas e os 15 hosts restantes se conetem a um segundo conjunto de portas. A profundidade da fila por porta é então reduzida para 15 x 128, ou seja, 1.920.
   - Opção 2:
     i. Designe cada host como "grande" ou "shopping" com base em sua necessidade de e/S esperada.
     ii. Multiplique o número de grandes iniciadores por 128.
     iii. Multiplique o número de pequenos iniciadores por 32.
     iv. Adicione os dois resultados juntos.
     v. Se o resultado for inferior a 2.048, defina a profundidade da fila para hosts grandes para 128 e a

profundidade da fila para hosts pequenos para 32.

vi. Se o resultado ainda for superior a 2.048 por porta, reduza a profundidade da fila por iniciador até que a profundidade total da fila seja inferior ou igual a 2.048.

> Para estimar a profundidade da fila necessária para obter uma determinada taxa de transferência de e/S por segundo, use esta fórmula:
>
> Profundidade da fila necessária (número de e/S por segundo) x (tempo de resposta)
>
> Por exemplo, se você precisar de 40.000 I/o por segundo com um tempo de resposta de 3 milissegundos, a profundidade de fila necessária é de 40.000 x (.003), ou seja, 120.

O número máximo de hosts que você pode se conetar a uma porta de destino é 64, se você decidir limitar a profundidade da fila à recomendação básica de 32. No entanto, se você decidir ter uma profundidade de fila de 128, então você pode ter um máximo de 16 hosts conetados a uma porta de destino. Quanto maior a profundidade da fila, menos hosts que uma única porta de destino pode suportar. Se sua exigência for tal que você não pode comprometer a profundidade da fila, então você deve obter mais portas de destino.

A profundidade de fila pretendida de 3.840 mm excede a profundidade de fila disponível por porta. Você tem 10 hosts grandes que têm altas necessidades de e/S de armazenamento e 20 hosts "shopping" que têm baixas necessidades de e/S. Defina a profundidade da fila do iniciador nos hosts grandes para 128 e a profundidade da fila do iniciador nos hosts pequenos para 32.

A profundidade total da fila resultante é de (10 x 128) (20 x 32) 1.920.

Você pode espalhar a profundidade da fila disponível igualmente em cada iniciador.

A profundidade da fila resultante por iniciador é de 2.048 ÷ 30 68.

Defina as profundidades da fila em hosts SAN

Talvez seja necessário alterar as profundidades da fila em seu host para alcançar os valores máximos de ITNs por nó e ventilador de porta FC.

AIX anfitriões

Você pode alterar a profundidade da fila em hosts AIX usando o `chdev` comando. As alterações feitas usando o `chdev` comando persistem nas reinicializações.

Exemplos:

- Para alterar a profundidade da fila do dispositivo hdisk7, use o seguinte comando:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Para alterar a profundidade da fila para o HBA fcs0, use o seguinte comando:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  O valor padrão para `num_cmd_elems` é 200. O valor máximo é 2.048.

Pode ser necessário colocar o HBA off-line para mudar `num_cmd_elems` e depois colocá-lo de volta on-line usando os `rmdev -l fcs0 -R` comandos e. `makdev -l fcs0 -P`

Hosts HP-UX

Você pode alterar a profundidade da fila de LUN ou dispositivo em hosts HP-UX usando o parâmetro kernel `scsi_max_qdepth` . Você pode alterar a profundidade da fila HBA usando o parâmetro kernel `max_fcp_reqs` .

- O valor padrão para `scsi_max_qdepth` é 8. O valor máximo é 255.

  `scsi_max_qdepth` pode ser alterado dinamicamente em um sistema em execução usando a `-u` opção no `kmtune` comando. A alteração será efetiva para todos os dispositivos no sistema. Por exemplo, use o seguinte comando para aumentar a profundidade da fila de LUN para 64:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  É possível alterar a profundidade da fila para arquivos de dispositivos individuais usando o `scsictl` comando. As alterações usando o `scsictl` comando não são persistentes em todas as reinicializações do sistema. Para exibir e alterar a profundidade da fila de um arquivo de dispositivo específico, execute o seguinte comando:

  ```
  scsictl -a /dev/rdsk/c2t2d0

  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- O valor padrão para `max_fcp_reqs` é 512. O valor máximo é 1024.

  O kernel deve ser reconstruído e o sistema deve ser reinicializado para que as alterações `max_fcp_reqs` entrem em vigor. Para alterar a profundidade da fila HBA para 256, por exemplo, use o seguinte comando:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Hosts Solaris

Você pode definir a profundidade da fila de LUN e HBA para seus hosts Solaris.

- Para a profundidade da fila de LUN: O número de LUNs em uso em um host multiplicado pelo acelerador por lun (profundidade da fila de lun) deve ser menor ou igual ao valor de profundidade da fila de tgt no host.
- Para a profundidade da fila em uma pilha Sun: Os drivers nativos não permitem configurações por LUN ou por destino `max_throttle` no nível HBA. O método recomendado para definir o `max_throttle` valor para drivers nativos está em um nível por tipo de dispositivo (VID_PID) nos `/kernel/drv/sd.conf` arquivos e `/kernel/drv/ssd.conf`. O utilitário de host define esse valor como 64 para configurações MPxIO e 8 para configurações Veritas DMP.

Passos

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. PESQUISE `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```

O valor padrão é definido como 32 na instalação.

4. Defina o valor desejado com base na configuração do seu ambiente.
5. Salve o arquivo.
6. Reinicie o host usando o `sync; sync; sync; reboot -- -r` comando.

Hosts VMware para um HBA QLogic

Use o `esxcfg-module` comando para alterar as configurações de tempo limite do HBA. A atualização manual do `esx.conf` ficheiro não é recomendada.

Passos

1. Faça logon no console de serviço como usuário raiz.
2. Use o `#vmkload_mod -l` comando para verificar qual módulo Qlogic HBA está atualmente carregado.
3. Para uma única instância de um Qlogic HBA, execute o seguinte comando:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

Este exemplo usa o módulo qla2300_707. Use o módulo apropriado com base na saída do `vmkload_mod -l`.

4. Salve suas alterações usando o seguinte comando:

```
#/usr/sbin/esxcfg-boot -b
```

5. Reinicie o servidor usando o seguinte comando:

```
#reboot
```

6. Confirme as alterações utilizando os seguintes comandos:
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Hosts VMware para um Emulex HBA

Use o `esxcfg-module` comando para alterar as configurações de tempo limite do HBA. A atualização manual do `esx.conf` ficheiro não é recomendada.

Passos

1. Faça logon no console de serviço como usuário raiz.
2. Use o `#vmkload_mod -l grep lpfc` comando para verificar qual Emulex HBA está atualmente carregado.
3. Para uma única instância de um Emulex HBA, digite o seguinte comando:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

Dependendo do modelo do HBA, o módulo pode ser lpfcdd_7xx ou lpfcdd_732. O comando acima usa o módulo lpfcdd_7xx. Você deve usar o módulo apropriado com base no resultado `vmkload_mod -l` do .

Executar este comando irá definir a profundidade da fila de LUN para 16 para o HBA representado por lpfc0.

4. Para várias instâncias de um Emulex HBA, execute o seguinte comando:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

A profundidade da fila LUN para lpfc0 e a profundidade da fila LUN para lpfc1 estão definidas para 16.

5. Introduza o seguinte comando:

```
#esxcfg-boot -b
```

6. Reinicie usando `#reboot`o .

Windows hosts para um Emulex HBA

Em hosts do Windows, você pode usar o `LPUTILNT` utilitário para atualizar a profundidade da fila para HBAs Emulex.

Passos

1. Execute o `LPUTILNT` utilitário localizado no `C:\WINNT\system32` diretório.
2. Selecione **Drive Parameters** no menu à direita.
3. Role para baixo e clique duas vezes em **QueueDepth**.

Se você estiver definindo **QueueDepth** maior que 150, o seguinte valor do Registro do Windows também precisará ser aumentado adequadamente:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

Hosts do Windows para um HBA Qlogic

Em hosts do Windows, você pode usar o `SANsurfer` utilitário gerenciador HBA para atualizar as profundidades da fila para HBAs Qlogic.

Passos

1. Execute o `SANsurfer` utilitário gerenciador HBA.
2. Clique em **HBA port** > **Settings**.
3. Clique em **Advanced HBA port settings** (Definições avançadas da porta HBA) na caixa de listagem.
4. Atualize `Execution Throttle` o parâmetro.

Hosts Linux para Emulex HBA

Você pode atualizar as profundidades da fila de um Emulex HBA em um host Linux. Para tornar as atualizações persistentes nas reinicializações, você deve criar uma nova imagem de disco RAM e reinicializar o host.

Passos

1. Identificar os parâmetros de profundidade da fila a modificar:

   ```
   modinfo lpfc|grep queue_depth
   ```

   É apresentada a lista de parâmetros de profundidade da fila com a respetiva descrição. Dependendo da versão do sistema operacional, você pode modificar um ou mais dos seguintes parâmetros de profundidade de fila:

   - `lpfc_lun_queue_depth`: Número máximo de comandos FC que podem ser enfileirados para um LUN específico (uint)
   - `lpfc_hba_queue_depth`: Número máximo de comandos FC que podem ser enfileirados para um HBA lpfc (uint)
   - `lpfc_tgt_queue_depth`: Número máximo de comandos FC que podem ser enfileirados para uma porta de destino específica (uint)

     O `lpfc_tgt_queue_depth` parâmetro é aplicável somente para sistemas Red Hat Enterprise Linux 7.x, sistemas SUSE Linux Enterprise Server 11 SP4 e sistemas 12.x.

2. Atualize as profundidades da fila adicionando os parâmetros de profundidade da fila ao `/etc/modprobe.conf` arquivo de um sistema Red Hat Enterprise Linux 5.x e ao `/etc/modprobe.d/scsi.conf` arquivo de um sistema Red Hat Enterprise Linux 6.x ou 7.x, ou de um sistema SUSE Linux Enterprise Server 11.x ou 12.x.

   Dependendo da versão do sistema operacional, você pode adicionar um ou mais dos seguintes comandos:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Crie uma nova imagem de disco RAM e reinicie o host para tornar as atualizações persistentes nas reinicializações.

   Para obter mais informações, consulte o "Administração do sistema" para sua versão do sistema operacional Linux.

4. Verifique se os valores de profundidade da fila são atualizados para cada parâmetro de profundidade da fila que você modificou:

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   É apresentado o valor atual da profundidade da fila.

Hosts Linux para QLogic HBA

Você pode atualizar a profundidade da fila de dispositivos de um driver QLogic em um host Linux. Para tornar as atualizações persistentes nas reinicializações, você deve criar uma nova imagem de disco RAM e reinicializar o host. Você pode usar a interface de linha de comando (CLI) do QLogic HBA para modificar a profundidade da fila do QLogic HBA.

Esta tarefa mostra como utilizar a CLI do QLogic HBA para modificar a profundidade da fila do QLogic HBA

Passos

1. Identificar o parâmetro de profundidade da fila do dispositivo a ser modificado:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   Você pode modificar apenas o `ql2xmaxqdepth` parâmetro de profundidade da fila, que indica a profundidade máxima da fila que pode ser definida para cada LUN. O valor padrão é 64 para RHEL 7,5 e posterior. O valor padrão é 32 para RHEL 7,4 e anterior.

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. Atualize o valor de profundidade da fila do dispositivo:

   - Se você quiser tornar as modificações persistentes, execute as seguintes etapas:
     i. Atualize as profundidades da fila adicionando o parâmetro profundidade da fila ao `/etc/modprobe.conf` arquivo para um sistema Red Hat Enterprise Linux 5.x e ao `/etc/modprobe.d/scsi.conf` arquivo para um sistema Red Hat Enterprise Linux 6.x ou 7.x, ou para um sistema SUSE Linux Enterprise Server 11.x ou 12.x: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. Crie uma nova imagem de disco RAM e reinicie o host para tornar as atualizações persistentes nas reinicializações.

     Para obter mais informações, consulte o "Administração do sistema" para sua versão do sistema operacional Linux.
   - Se você quiser modificar o parâmetro somente para a sessão atual, execute o seguinte comando:

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     No exemplo a seguir, a profundidade da fila é definida como 128.

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. Verifique se os valores de profundidade da fila estão atualizados:

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

   É apresentado o valor atual da profundidade da fila.

4. Modifique a profundidade da fila do QLogic HBA atualizando o parâmetro do firmware `Execution Throttle` a partir do BIOS do QLogic HBA.

   a. Inicie sessão na CLI de gestão do QLogic HBA:

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. No menu principal, selecione a `Adapter Configuration` opção.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

   c. Na lista de parâmetros de configuração do adaptador, selecione a `HBA Parameters` opção.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Na lista de portas HBA, selecione a porta HBA necessária.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

São apresentados os detalhes da porta HBA.

e. No menu HBA Parameters (parâmetros HBA), selecione a `Display HBA Parameters` opção para visualizar o valor atual `Execution Throttle` da opção.

O valor padrão da `Execution Throttle` opção é 65535.

```
HBA Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-----------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-----------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Pressione **Enter** para continuar.

b. No menu HBA Parameters (parâmetros HBA), selecione a `Configure HBA Parameters` opção para modificar os parâmetros HBA.

c. No menu Configurar parâmetros, selecione a `Execute Throttle` opção e atualize o valor deste parâmetro.

```
Configure Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Pressione **Enter** para continuar.

e. No menu Configurar parâmetros, selecione a `Commit Changes` opção para guardar as alterações.

f. Saia do menu.

S3 gerenciamento de storage de objetos

Saiba mais sobre o suporte S3 no ONTAP 9

Saiba mais sobre a configuração do ONTAP S3

A partir do ONTAP 9.8, é possível habilitar um servidor de storage de objetos do ONTAP Simple Storage Service (S3) em um cluster ONTAP, usando ferramentas conhecidas de gerenciabilidade, como o Gerenciador de sistemas ONTAP, para provisionar rapidamente o storage de objetos de alta performance para desenvolvimento e operações no ONTAP, aproveitando as eficiências de storage e a segurança do ONTAP.

Configuração do S3 com o Gerenciador de sistemas e a CLI do ONTAP

Você pode configurar e gerenciar o ONTAP S3 com o Gerenciador de sistema e a CLI do ONTAP. Quando você ativa o S3 e cria buckets usando o Gerenciador do sistema, o ONTAP seleciona padrões de práticas recomendadas para configuração simplificada. Se você precisar especificar parâmetros de configuração, talvez queira usar a CLI do ONTAP. Se você configurar o servidor S3 e os buckets da CLI, ainda poderá gerenciá-los com o System Manager, se desejado, ou vice-versa.

Quando você cria um bucket do S3 usando o Gerenciador do sistema, o ONTAP configura um nível de serviço de desempenho padrão que é o mais alto disponível no sistema. Por exemplo, em um sistema AFF, a configuração padrão seria **Extreme**. Os níveis de serviço de performance são grupos de políticas de qualidade do serviço (QoS) adaptáveis predefinidos. Em vez de um dos níveis de serviço padrão, você pode especificar um grupo de políticas de QoS personalizado ou nenhum grupo de políticas.

Os grupos de políticas de QoS adaptáveis predefinidos são:

- **Extreme**: Usado para aplicativos que esperam a menor latência e o mais alto desempenho.
- **Desempenho**: Usado para aplicativos com necessidades de desempenho modestas e latência.
- **Valor**: Usado para aplicativos para os quais a taxa de transferência e a capacidade são mais importantes do que a latência.
- **Custom**: Especifique uma política de QoS personalizada ou nenhuma política de QoS.

Se você selecionar **Use for Tiering**, nenhum nível de serviço de desempenho será selecionado e o sistema tentará selecionar Mídia de baixo custo com desempenho ideal para os dados em camadas.

Veja também"Use grupos de políticas de QoS adaptáveis": .

A ONTAP tenta provisionar esse bucket em camadas locais que tenham os discos mais apropriados, atendendo ao nível de serviço escolhido. No entanto, se você precisar especificar quais discos incluir no bucket, considere configurar o armazenamento de objetos S3 a partir da CLI especificando os níveis locais (agregado). Se você configurar o servidor S3 a partir da CLI, ainda poderá gerenciá-lo com o System Manager, se desejado.

Se você quiser a capacidade de especificar quais agregados são usados para buckets, você só pode fazer isso usando a CLI.

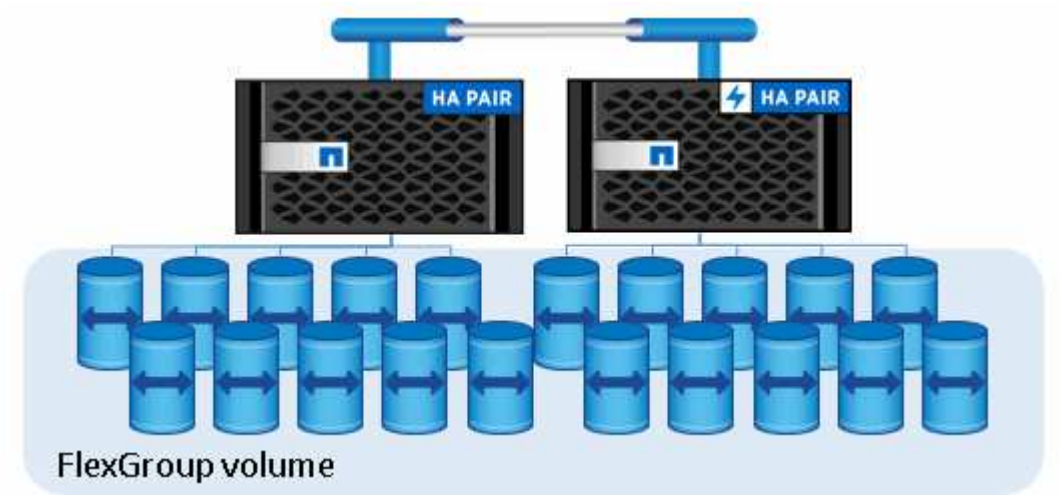
Configurando buckets do S3 no Cloud Volumes ONTAP

Se você quiser atender buckets do Cloud Volumes ONTAP, é altamente recomendável que você selecione manualmente os agregados subjacentes para garantir que eles estejam usando apenas um nó. O uso de agregados de ambos os nós pode afetar o desempenho, porque os nós estarão em zonas de disponibilidade geograficamente separadas e, portanto, suscetíveis a problemas de latência. Portanto, em ambientes Cloud Volumes ONTAP, você deve Configurar buckets do S3 a partir da CLI.

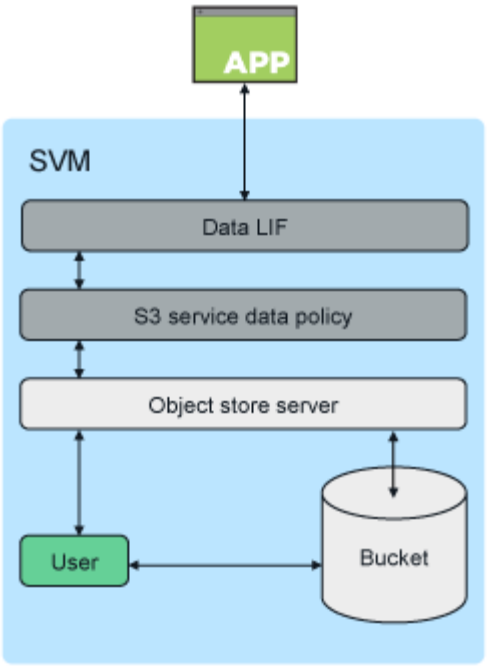
Caso contrário, os servidores S3 no Cloud Volumes ONTAP são configurados e mantidos da mesma forma no Cloud Volumes ONTAP que em ambientes locais.

Arquitetura do ONTAP S3 usando o FlexGroup volumes

No ONTAP, a arquitetura subjacente para um bucket é um "Volume FlexGroup", que é um namespace único que é composto por vários volumes de membros constituintes, mas é gerenciado como um único volume.



O acesso ao bucket é fornecido por meio de usuários autorizados e aplicativos clientes.



Quando um bucket é usado exclusivamente para aplicativos S3, incluindo o uso como um endpoint FabricPool, o volume FlexGroup subjacente só suportará o protocolo S3.

A partir do ONTAP 9.12,1, o protocolo S3 também pode ser ativado em "Volumes nas multiprotocolo" que foram pré-configurados para usar protocolos nas. Quando o protocolo S3 está habilitado em volumes nas multiprotocolo, as aplicações clientes podem ler e gravar dados usando NFS, SMB e S3.

Limites do balde

O tamanho mínimo do balde é 95GB. O tamanho máximo do balde é limitado ao tamanho máximo de FlexGroup de 60PB.

Há um limite de 1000 buckets por volume do FlexGroup ou 12.000 buckets por cluster (usando volumes do FlexGroup de 12 GB).

Dimensionamento automático de FlexGroup com ONTAP 9.14,1 e posterior

A partir do ONTAP 9.14,1, o tamanho padrão do FlexGroup é baseado no tamanho dos buckets subjacentes. O volume FlexGroup aumentará ou diminuirá automaticamente à medida que os baldes forem adicionados ou removidos.

Por exemplo, se um bucket_A inicial for provisionado para ser 100GB, o FlexGroup será thin-provisionado para ser 100GB. Se forem criados dois buckets adicionais, Bucket_B a 300GB e Bucket_C a 500GB, o volume FlexGroup aumentará para 900GB.

(Bucket_a a 100GB Bucket_B a 300GB Bucket_C a 500GB 900GB.)

Se Bucket_A for excluído, o volume FlexGroup subjacente será reduzido para 800GB.

Tamanhos de FlexGroup padrão corrigidos no ONTAP 9.13,1 e anteriores

Para fornecer capacidade para expansão do bucket, a capacidade total usada de todos os buckets no volume

FlexGroup deve ser inferior a 33% da capacidade máxima de volume FlexGroup com base em agregados de storage disponíveis no cluster. Se isso não puder ser atendido, o novo bucket que está sendo criado será provisionado em um novo volume FlexGroup criado automaticamente.

Antes do ONTAP 9.14,1, o tamanho do FlexGroup é fixado a um tamanho padrão com base em seu ambiente:

- 1,6PB em ONTAP
- 100TB em ONTAP Select

Se um cluster não tiver capacidade suficiente para provisionar um volume FlexGroup no tamanho padrão, o ONTAP reduzirá o tamanho padrão pela metade até que ele possa ser provisionado no ambiente existente.

Por exemplo, em um ambiente 300TB, um volume FlexGroup é provisionado automaticamente a 200TB TB (volumes FlexGroup de 1,6PB TB, 800TB TB e 400TB TB sendo muito grandes para o ambiente).

ONTAP S3 principais casos de uso

Estes são os principais casos de uso para acesso de cliente aos serviços do ONTAP S3:

- Usando o FabricPool para categorizar dados inativos em um bucket no ONTAP, permitindo que a ONTAP disponha em camadas do ONTAP. A disposição em camadas em um bucket no "cluster local"repositório ou a disposição em camadas em um bucket no repositório "cluster remoto"é compatível. A disposição em camadas no ONTAP S3 permite que você use sistemas ONTAP mais baratos para dados inativos e economize dinheiro com uma nova capacidade flash, sem a necessidade de licenças FabricPool adicionais ou novas tecnologias para gerenciar.
- A partir do ONTAP 9.12,1, o protocolo S3 também pode ser ativado em "Volumes nas multiprotocolo" que foram pré-configurados para usar protocolos nas. Quando o protocolo S3 está habilitado em volumes nas multiprotocolo, as aplicações clientes podem ler e gravar dados usando S3, NFS e SMB, o que abre uma variedade de casos de uso adicionais. Um dos casos de uso mais comuns são os clientes nas que gravam dados em um volume e os clientes S3 que leem os mesmos dados e executam tarefas especializadas, como análise, business intelligence, aprendizado de máquina e reconhecimento ótico de carateres.

> O ONTAP S3 é apropriado se você quiser habilitar os recursos do S3 em clusters ONTAP existentes sem hardware e gerenciamento adicionais. O NetApp StorageGRID é a principal solução da NetApp para armazenamento de objetos. O StorageGRID é recomendado para aplicações S3 nativas que precisam aproveitar toda a gama de ações S3, recursos avançados de ILM ou capacidades não alcançáveis em sistemas baseados em ONTAP. Para obter mais informações, consulte "Documentação do StorageGRID".

Informações relacionadas

"Gerenciamento de volumes do FlexGroup"

Plano

Versão do ONTAP e suporte de plataforma para storage de objetos S3

O storage de objetos do S3 é compatível com todas as plataformas AFF, FAS e ONTAP Select usando o ONTAP 9.8 e posterior.

Assim como em outros protocolos, como FC, iSCSI, NFS, NVMe_of e SMB, o S3 requer a instalação de uma licença antes que ela possa ser usada no ONTAP. A licença S3 é uma licença de custo zero, mas deve ser

instalada em sistemas que estejam atualizando para o ONTAP 9.8. A licença S3 pode ser transferida a partir do "Página chaves de licença principal"no site de suporte da NetApp.

Os novos sistemas ONTAP 9.8 e posteriores têm a licença S3 pré-instalada.

Cloud Volumes ONTAP

O ONTAP S3 é configurado e funciona da mesma forma no Cloud Volumes ONTAP que em ambientes locais, com uma exceção:

- Ao criar buckets no Cloud Volumes ONTAP, você deve usar o procedimento de CLI para garantir que o volume FlexGroup subjacente use apenas agregados de um único nó. O uso de agregados de vários nós afetará o desempenho porque os nós estarão em zonas de disponibilidade geograficamente separadas e suscetíveis a problemas de latência.

Fornecedor de nuvem	Versão de ONTAP
Azure	ONTAP 9.9,1 e posterior
AWS	ONTAP 9.11,0 e posterior
Google Cloud	ONTAP 9.12,1 e posterior

Amazon FSX para NetApp ONTAP

O armazenamento de objetos S3 é compatível com os serviços do Amazon FSX for NetApp usando o ONTAP 9.11 e posterior.

Suporte S3 com MetroCluster

A partir do ONTAP 9.14,1, é possível habilitar um servidor de storage de objetos S3 em uma SVM em um agregado espelhado em configurações IP e FC do MetroCluster.

A partir do ONTAP 9.12,1, é possível habilitar um servidor de storage de objetos S3 em uma SVM em um agregado sem espelhamento em uma configuração IP do MetroCluster. Para obter mais informações sobre as limitações de agregados sem espelhamento em configurações MetroCluster IP, "Considerações para agregados sem espelhamento"consulte .

S3 visualização pública no ONTAP 9.7

No ONTAP 9.7, o armazenamento de objetos S3 foi introduzido como uma prévia pública. Essa versão não foi destinada a ambientes de produção e não será mais atualizada a partir do ONTAP 9.8. Somente as versões do ONTAP 9.8 e posteriores são compatíveis com storage de objetos do S3 em ambientes de produção.

Os buckets do S3 criados com a visualização pública do 9,7 podem ser usados no ONTAP 9.8 e posterior, mas não podem aproveitar os aprimoramentos de recursos. Se você tiver buckets criados com a visualização pública do 9,7, migre o conteúdo desses buckets para buckets do 9,8 para oferecer suporte a recursos, segurança e melhorias de desempenho.

Ações compatíveis com o ONTAP S3

As ações do ONTAP S3 são compatíveis com APIs REST S3 padrão, exceto conforme indicado abaixo. Para obter detalhes, consulte "Referência de API do Amazon S3".

Operações do balde

As operações a seguir são suportadas no ONTAP usando APIs AWS S3:

Funcionamento do balde	Suporte ONTAP começando com
CreateBucket	ONTAP 9.11,1
DeleteBucket	ONTAP 9.11,1
DeleteBucketPolicy	ONTAP 9.12,1
GetBucketAcl	ONTAP 9,8
GetBucketLifecycleConfiguration	ONTAP 9.13,1 * apenas ações de expiração são suportadas
GetBucketlocalização	ONTAP 9.10,1
Política de GetBucketPolicy	ONTAP 9.12,1
Balde para a cabeça	ONTAP 9,8
ListBuckets	ONTAP 9,8
ListBucketControle de versão	ONTAP 9.11,1
ListObjectVersions	ONTAP 9.11,1
PutBucket	• ONTAP 9.11,1 • ONTAP 9.8 - compatível apenas com APIs REST do ONTAP
PutBucketLifecycleConfiguration	ONTAP 9.13,1 * apenas ações de expiração são suportadas
Política de PutBucketPolicy	ONTAP 9.12,1

Operações de objetos

A partir do ONTAP 9.9,1, o ONTAP S3 oferece suporte a metadados e marcação de objetos.

- PutObject e CreateMultipartUpload incluem pares de chave-valor usando `x-amz-meta-<key>.`

  Por exemplo `x-amz-meta-project: ontap_s3:.`

- GetObject. E HeadObject retornam metadados definidos pelo usuário.
- Ao contrário dos metadados, as tags podem ser lidas independentemente dos objetos usando:
  - Marcação de objetos
  - GetObjectTagging
  - DeleteObjectTagging

A partir do ONTAP 9.11,1, o ONTAP S3 oferece suporte ao controle de versão de objetos e às ações associadas a essas APIs do ONTAP:

- GetBucketControle de versão

- ListBucketVersions
- PutBucketControle de versão

Operação do objeto	Suporte ONTAP começando com
AbortMultipartUpload	ONTAP 9,8
CompleteMultipartUpload	ONTAP 9,8
CopyObject	ONTAP 9.12,1
CreateMultipartUpload	ONTAP 9,8
DeleteObject	ONTAP 9,8
DeleteObjects	ONTAP 9.11,1
DeleteObjectTagging	ONTAP 9.9,1
GetBucketControle de versão	ONTAP 9.11,1
GetObject	ONTAP 9,8
GetObjectAcl	ONTAP 9,8
GetObjectRetention	ONTAP 9.14,1
GetObjectTagging	ONTAP 9.9,1
HeadObject	ONTAP 9,8
ListMultipartUpload	ONTAP 9,8
ListObjects	ONTAP 9,8
ListObjectsV2	ONTAP 9,8
ListBucketVersions	ONTAP 9.11,1
ListParts	ONTAP 9,8
PutBucketControle de versão	ONTAP 9.11,1
PutObject	ONTAP 9,8
PutObjectLockConfiguration	ONTAP 9.14,1
Retenção PutObjectRetention	ONTAP 9.14,1
Marcação de objetos	ONTAP 9.9,1
UploadPart	ONTAP 9,8
UploadPartCopy	ONTAP 9.12,1

Políticas de grupo

Essas operações não são específicas do S3 e geralmente estão associadas a processos de identidade e gerenciamento (IAM). O ONTAP é compatível com esses comandos, mas não usa as APIs REST do IAM.

- Criar política
- Política do AttachGroup

Gerenciamento de usuários

Essas operações não são específicas do S3 e geralmente estão associadas aos processos do IAM.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

S3 ações por liberação

ONTAP 9.14,1

ONTAP 9.14,1 adiciona suporte para bloqueio de objetos S3.

> Operações de retenção legal (bloqueios sem tempos de retenção definidos) não são suportadas.

- GetObjectLockConfiguration
- GetObjectRetention
- PutObjectLockConfiguration
- Retenção PutObjectRetention

ONTAP 9.13,1

O ONTAP 9.13,1 adiciona suporte ao gerenciamento do ciclo de vida do bucket.

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9.12,1

O ONTAP 9.12,1 adiciona suporte a políticas de bucket e a capacidade de copiar objetos.

- DeleteBucketPolicy
- Política de GetBucketPolicy
- Política de PutBucketPolicy
- CopyObject
- UploadPartCopy

ONTAP 9.11,1

O ONTAP 9.11,1 adiciona suporte para versionamento, URLs pré-assinados, uploads em grupo e suporte para ações S3 comuns, como criar e excluir buckets usando APIs do S3.

- O ONTAP S3 agora suporta pedidos de assinatura de uploads em pedaços usando x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD
- O ONTAP S3 agora oferece suporte a aplicativos clientes usando URLs pré-assinados para compartilhar objetos ou permitir que outros usuários façam upload de objetos sem exigir credenciais de usuário.
- CreateBucket

- DeleteBucket
- GetBucketControle de versão
- ListBucketVersions
- PutBucket
- PutBucketControle de versão
- DeleteObjects
- ListObjectVersions

Como o FlexGroup subjacente não é criado até que o primeiro bucket seja, um bucket deve ser criado no ONTAP antes que um cliente externo possa criar um bucket usando o CreateBucket.

ONTAP 9.10,1

ONTAP 9.10,1 adiciona suporte para SnapMirror S3 e GetBucketLocation.

- GetBucketlocalização

ONTAP 9.9,1

O ONTAP 9.9,1 adiciona suporte para metadados de objetos e suporte a marcação ao ONTAP S3.

- PutObject e CreateMultipartUpload agora incluem pares de chave-valor usando 'x-amz-meta-<key>'. Por exemplo: 'X-amz-meta-project: ONTAP_S3'.
- GetObject e HeadObject agora retornam metadados definidos pelo usuário.

Tags também podem ser usadas com baldes. Ao contrário dos metadados, as tags podem ser lidas independentemente dos objetos usando:

- Marcação de objetos
- GetObjectTagging
- DeleteObjectTagging

Interoperabilidade do ONTAP S3

O servidor ONTAP S3 interage normalmente com outras funcionalidades do ONTAP, exceto conforme indicado nesta tabela.

Área da função	Suportado	Não suportado
Cloud Volumes ONTAP	• Clientes Azure no ONTAP 9.9,1 e versões posteriores • Clientes da AWS no ONTAP 9.11,0 e versões posteriores • Clientes do Google Cloud no ONTAP 9.12,1 e versões posteriores	• Cloud Volumes ONTAP para qualquer cliente no ONTAP 9.8 e versões anteriores

Área da função	Suportado	Não suportado
Proteção de dados	• Cloud Sync • Bloqueio de objetos; governança e conformidade (começando com ONTAP 9.14,1) • "Controle de versão do objeto" (Começando com ONTAP 9.11,1) • Agregados MetroCluster não espelhados (começando com ONTAP 9.12,1) • Agregados MetroCluster espelhados (começando com ONTAP 9.14,1) • "SnapMirror S3" (Começando com ONTAP 9.10,1) • SnapMirror (somente volumes nas; começando com ONTAP 9.12,1) • SnapLock (somente volumes nas; começando com ONTAP 9.14,1)	• Codificação de apagamento • NDMP • SMTape • SnapMirror • Nuvem da SnapMirror • Recuperação de desastres da SVM • SyncMirror
Criptografia	• Criptografia de agregados NetApp (NAE) • Criptografia de volume NetApp (NVE) • Criptografia de storage do NetApp (NSE) • TLS/SSL	• ESCÓRIA
Eficiência de storage	• Deduplicação • Compactação • Compactação	• Eficiências de nível de agregado • Clone de volume do volume FlexGroup que contém buckets do ONTAP S3
Virtualização de storage	-	Virtualização NetApp FlexArray
Qualidade do serviço (QoS)	• Valores máximos de QoS (tetos) • Mínimos de QoS (andares)	-

Área da função	Suportado	Não suportado
Recursos adicionais	• "Auditoria S3 eventos" (Começando com ONTAP 9.10,1) • "Gerenciamento do ciclo de vida do bucket" (Começando com ONTAP 9.13,1)	• Volumes FlexCache • FPolicy • Qtrees • Quotas

As soluções de terceiros recomendadas pela NetApp para o bucket do ONTAP S3

A NetApp validou as seguintes soluções de terceiros para uso com o ONTAP S3. Se a solução que você está procurando não estiver listada, entre em Contato com seu representante da conta do NetApp.

Soluções de terceiros validadas no ONTAP S3

A NetApp testou essas soluções em colaboração com os respetivos parceiros.

- Amazon SageMaker
- Cliente Apache Hadoop S3A
- Apache Kafka
- Kit de proteção (V11)
- Kafka fluente
- Red Hat Quay
- Rubrik
- Floco de neve
- Trino
- Kit de meia (V12)

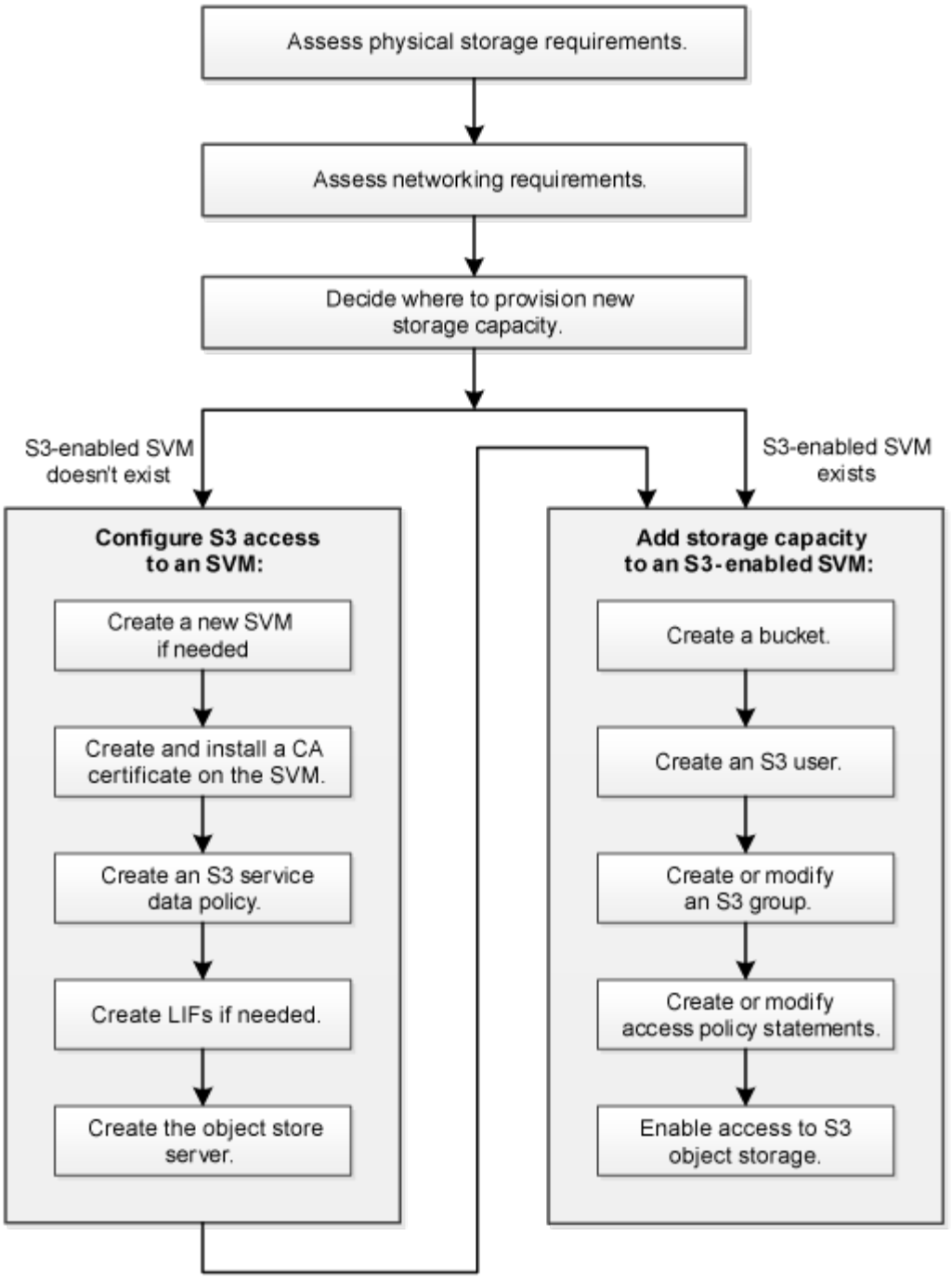
Configurar

Sobre o processo de configuração do S3

Fluxo de trabalho de configuração do ONTAP S3

A configuração do S3 envolve a avaliação dos requisitos de storage físico e rede e, depois, a escolha de um fluxo de trabalho específico para sua meta: Configurar o acesso do S3 a um SVM novo ou existente, ou adicionar um bucket e usuários a um SVM existente que já esteja totalmente configurado para o acesso S3.

Ao configurar o acesso S3 a uma nova VM de armazenamento usando o System Manager, você será solicitado a inserir informações de certificado e rede, e a VM de armazenamento e o servidor de armazenamento de objetos S3 são criados em uma única operação.



Avaliar os requisitos de storage físico do ONTAP S3

Antes de provisionar o storage S3 para clientes, você deve garantir que haja espaço suficiente em agregados existentes para o novo armazenamento de objetos. Se não houver, você poderá adicionar discos a agregados existentes ou criar novos agregados do tipo e local desejados.

Sobre esta tarefa

Quando você cria um bucket do S3 em um SVM habilitado para S3, um volume do FlexGroup é "criado automaticamente"compatível com o bucket. Você pode permitir ao ONTAP Select os agregados subjacentes e componentes do FlexGroup automaticamente (o padrão) ou selecionar os agregados subjacentes e componentes do FlexGroup você mesmo.

Se você decidir especificar os agregados e componentes do FlexGroup — por exemplo, se você tiver requisitos de desempenho específicos para os discos subjacentes — você deve garantir que sua configuração agregada esteja de acordo com as diretrizes de práticas recomendadas para o provisionamento de um volume FlexGroup. Saiba mais:

- "Gerenciamento de volumes do FlexGroup"
- "Relatório técnico da NetApp 4571-a: Melhores práticas de volume da NetApp ONTAP FlexGroup"

Se você estiver atendendo buckets do Cloud Volumes ONTAP, é altamente recomendável que você selecione manualmente os agregados subjacentes para garantir que eles estejam usando apenas um nó. O uso de agregados de ambos os nós pode afetar o desempenho, porque os nós estarão em zonas de disponibilidade geograficamente separadas e, portanto, suscetíveis a problemas de latência. Saiba mais "Criando buckets para Cloud Volumes ONTAP"sobre .

Você pode usar o servidor ONTAP S3 para criar uma camada de capacidade FabricPool local, ou seja, no mesmo cluster que a camada de performance. Isso pode ser útil, por exemplo, se você tiver discos SSD conetados a um par de HA e quiser categorizar dados *cold* em discos HDD em outro par de HA. Nesse caso de uso, o servidor S3 e o bucket que contém o nível de capacidade local devem, portanto, estar em um par de HA diferente do nível de performance. A disposição em camadas local não é compatível com clusters de um ou dois nós.

Passos

1. Exibir espaço disponível em agregados existentes:

   ```
   storage aggregate show
   ```

   Se houver um agregado com espaço suficiente ou localização do nó necessária, Registre seu nome para sua configuração do S3.

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. Se não houver agregados com espaço suficiente ou localização de nó necessária, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede do ONTAP S3

Antes de fornecer armazenamento S3 para clientes, você deve verificar se a rede está corretamente configurada para atender aos requisitos de provisionamento S3.

Antes de começar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)
- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Sobre esta tarefa

Para camadas remotas de capacidade FabricPool (nuvem) e clientes S3 remotos, você precisa usar um SVM de dados e configurar LIFs de dados. Para camadas de nuvem do FabricPool, você também precisa configurar LIFs entre clusters. O peering de cluster não é necessário.

Para níveis de capacidade locais do FabricPool, você precisa usar o SVM do sistema (chamado de "'cluster'"), mas você tem duas opções de configuração de LIF:

- Você pode usar os LIFs de cluster.

  Nesta opção, não é necessária nenhuma configuração de LIF adicional, mas haverá um aumento no tráfego nos LIFs de cluster. Além disso, o nível local não será acessível a outros clusters.

- Você pode usar dados e LIFs entre clusters.

  Essa opção requer configuração adicional, incluindo a ativação das LIFs para o protocolo S3, mas o nível local também estará acessível como uma camada de nuvem FabricPool remota para outros clusters.

Passos

1. Exiba as portas físicas e virtuais disponíveis:

   ```
   network port show
   ```

   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.
   - Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis:

   ```
   network subnet show
   ```

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis:

   ```
   network ipspace show
   ```

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster:

   ```
   network options ipv6 show
   ```

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decidir onde provisionar nova capacidade de storage ONTAP S3

Antes de criar um novo bucket do S3, você deve decidir se o colocará em um SVM novo ou existente. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um bucket em um novo SVM ou SVM que não esteja habilitado para S3, execute as etapas dos tópicos a seguir.

  "Criar um SVM para S3"

  "Crie um bucket para S3"

  Embora o S3 possa coexistir em uma SVM com NFS e SMB, você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

  - Você está habilitando S3 em um cluster pela primeira vez.
  - Você tem SVMs existentes em um cluster no qual não deseja habilitar o suporte ao S3.
  - Você tem um ou mais SVMs habilitados para S3 em um cluster e deseja outro servidor S3 com caraterísticas de desempenho diferentes. Depois de ativar o S3 no SVM, prossiga com o provisionamento de um bucket.

- Se você quiser provisionar o bucket inicial ou um bucket adicional em um SVM habilitado para S3 existente, execute as etapas do tópico a seguir.

  "Crie um bucket para S3"

Configurar o acesso do S3 a uma SVM

Criar um SVM para ONTAP S3

Embora o S3 possa coexistir com outros protocolos em um SVM, você pode querer criar um novo SVM para isolar o namespace e a carga de trabalho.

Sobre esta tarefa

Se você estiver fornecendo apenas um storage de objetos S3 a partir de uma SVM, o servidor S3 não exigirá nenhuma configuração DNS. No entanto, você pode querer configurar o DNS no SVM se outros protocolos forem usados.

Ao configurar o acesso S3 a uma nova VM de armazenamento usando o System Manager, você será

solicitado a inserir informações de certificado e rede, e a VM de armazenamento e o servidor de armazenamento de objetos S3 são criados em uma única operação.

Exemplo 20. Passos

System Manager

Você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN do servidor S3 não deve começar com um nome de bucket.

Você deve estar preparado para inserir endereços IP para dados de função de interface.

Se você estiver usando um certificado assinado de CA externo, será solicitado que o insira durante este procedimento; você também terá a opção de usar um certificado gerado pelo sistema.

1. Habilite o S3 em uma VM de storage.

   a. Adicionar uma nova VM de armazenamento: Clique em **armazenamento > armazenamento de VMs** e, em seguida, clique em **Adicionar**.

      Se este for um novo sistema sem VMs de armazenamento existentes: Clique em **Dashboard > Configure Protocols**.

   Se estiver adicionando um servidor S3 a uma VM de armazenamento existente: Clique em **armazenamento > armazenamento de VMs**, selecione uma VM de armazenamento, clique em **Configurações** e, em seguida, clique em **S3**.

   a. Clique em **Ativar S3** e, em seguida, introduza o nome do servidor S3.
   b. Selecione o tipo de certificado.

      Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.

   c. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Verifique se o S3 está licenciado no cluster:

   ```
   system license show -package s3
   ```

   Se não estiver, contacte o seu representante de vendas.

2. Criar um SVM:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- Utilize a definição UNIX para a `-rootvolume-security-style` opção.
- Utilize a opção C.UTF-8 predefinida `-language`.
- A `ipspace` definição é opcional.

3. Verifique a configuração e o status do SVM recém-criado:

```
vserver show -vserver <svm_name>
```

O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no ipspace ipspaceA:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação. Por padrão, a conta de usuário vsadmin é criada e está no `locked` estado. A função vsadmin é atribuída à conta de usuário padrão vsadmin.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                       Vserver Admin State: running
                 Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Crie e instale um certificado de CA em um SVM habilitado para ONTAP S3

Um certificado de autoridade de certificação (CA) é necessário para habilitar o tráfego HTTPS de clientes S3 para o SVM habilitado para S3. O uso de certificados de CA cria uma relação confiável entre aplicativos clientes e o servidor de armazenamento de objetos ONTAP. Um certificado de CA deve ser instalado no ONTAP antes de usá-lo como um armazenamento de objetos acessível a clientes remotos.

Sobre esta tarefa

Embora seja possível configurar um servidor S3 para usar apenas HTTP, e embora seja possível configurar clientes sem um requisito de certificado de CA, é uma prática recomendada proteger o tráfego HTTPS para servidores ONTAP S3 com um certificado de CA.

Um certificado de CA não é necessário para um caso de uso local de disposição em camadas, em que o tráfego IP está passando apenas pelas LIFs de cluster.

As instruções neste procedimento irão criar e instalar um certificado auto-assinado ONTAP. Embora o ONTAP possa gerar certificados autoassinados, o uso de certificados assinados de uma autoridade de certificação de terceiros é a prática recomendada.; consulte a documentação de autenticação do administrador para obter mais informações.

"Autenticação de administrador e RBAC"

Consulte as `security certificate` páginas man para obter opções de configuração adicionais.

Passos

1. Crie um certificado digital autoassinado:

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   A `-type root-ca` opção cria e instala um certificado digital autoassinado para assinar outros certificados agindo como autoridade de certificação (CA).

   A `-common-name` opção cria o nome da Autoridade de Certificação (CA) do SVM e será usada ao gerar o nome completo do certificado.

   O tamanho padrão do certificado é de 2048 bits.

   Exemplo

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Quando o nome gerado do certificado for exibido; certifique-se de salvá-lo para etapas posteriores neste procedimento.

2. Gerar uma solicitação de assinatura de certificado:

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   O `-common-name` parâmetro para a solicitação de assinatura deve ser o nome do servidor S3 (FQDN).

   Você pode fornecer a localização e outras informações detalhadas sobre o SVM, se desejado.

   Você será solicitado a manter uma cópia da solicitação de certificado e da chave privada para referência futura.

3. Assine a CSR usando SVM_CA para gerar o certificado do S3 Server:

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   Insira as opções de comando que você usou nas etapas anteriores:

   - `-ca` — o nome comum da CA que você inseriu na Etapa 1.
   - `-ca-serial` — o número de série da CA a partir do passo 1. Por exemplo, se o nome do certificado CA for svm1_CA_159D1587CE21E9D4_svm1_CA, o número de série será 159D1587CE21E9D4.

Por padrão, o certificado assinado expirará em 365 dias. Você pode selecionar outro valor e especificar outros detalhes de assinatura.

Quando solicitado, copie e insira a string de solicitação de certificado que você salvou na Etapa 2.

Um certificado assinado é exibido; salve-o para uso posterior.

4. Instale o certificado assinado no SVM habilitado para S3:

   `security certificate install -type server -vserver svm_name`

   Quando solicitado, insira o certificado e a chave privada.

   Você tem a opção de inserir certificados intermediários se uma cadeia de certificados for desejada.

   Quando a chave privada e o certificado digital assinado pela CA forem exibidos, salve-os para referência futura.

5. Obtenha o certificado de chave pública:

   `security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

   Salve o certificado de chave pública para uma configuração posterior do lado do cliente.

   Exemplo

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
          FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
               Certificate Authority: svm1_ca
                 Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
             Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
              Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                           Protocol: SSL
                     Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Crie a política de dados de serviço do ONTAP S3

Você pode criar políticas de serviço para dados e serviços de gerenciamento do S3. É necessária uma política de dados de serviço S3 para permitir o tráfego de dados S3 nos LIFs.

Sobre esta tarefa

Uma política de dados de serviço S3 é necessária se você estiver usando LIFs de dados e LIFs entre clusters. Não é necessário se você estiver usando LIFs de cluster para o caso de uso de disposição em camadas local.

Quando uma política de serviço é especificada para um LIF, a política é usada para criar uma função padrão, política de failover e lista de protocolos de dados para o LIF.

Embora vários protocolos possam ser configurados para SVMs e LIFs, é uma prática recomendada para S3 ser o único protocolo ao fornecer dados de objetos.

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Criar uma política de dados de serviço:

   `network interface service-policy create -vserver` *`svm_name`* `-policy` *`policy_name`* `-services data-core,data-s3-server`

   Os `data-core` serviços e `data-s3-server` são os únicos necessários para habilitar o ONTAP S3, embora outros serviços possam ser incluídos conforme necessário.

Criar LIFs de dados para o ONTAP S3

Se você criou um novo SVM, as LIFs dedicadas que você cria para o acesso S3 devem ser LIFs de dados.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- A política de serviço LIF já deve existir.
- Como prática recomendada, os LIFs usados para acesso a dados (data-S3-server) e LIFs usados para operações de gerenciamento (Management-https) devem ser separados. Ambos os serviços não devem ser ativados no mesmo LIF.
- Os Registros DNS devem ter apenas endereços IP dos LIFs que têm dados-S3-server associados a eles. Se endereços IP de outros LIFs forem especificados no Registro DNS, as solicitações do ONTAP S3 podem ser atendidas por outros servidores, resultando em respostas inesperadas ou perda de dados.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- Se você habilitar a disposição em camadas remota de capacidade FabricPool (nuvem), também deverá configurar LIFs entre clusters.

Passos

1. Criar um LIF:

   `network interface create -vserver` *`svm_name`* `-lif` *`lif_name`* `-service-policy` *`service_policy_names`* `-home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto-revert {true|false}`

   - `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

     Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial

com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.
- A `-service-policy` opção especifica a política de dados e serviços de gerenciamento que você criou e quaisquer outras políticas necessárias.

2. Se você quiser atribuir um endereço IPv6 na `-address` opção:

   a. Use o `network ndp prefix show` comando para visualizar a lista de prefixos RA aprendidos em várias interfaces.

      O `network ndp prefix show` comando está disponível no nível de privilégio avançado.

   b. Use o formato `prefix:id` para construir o endereço IPv6 manualmente.

      `prefix` é o prefixo aprendido em várias interfaces.

   Para derivar o `id`, escolha um número hexadecimal aleatório de 64 bits.

3. Verifique se o LIF foi criado com sucesso usando o `network interface show` comando.
4. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Exemplos

O comando a seguir mostra como criar um LIF de dados S3 atribuído com a `my-S3-policy` política de serviço:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Criar LIFs entre clusters para disposição remota de FabricPool em camadas com o ONTAP S3

Se você estiver habilitando a disposição em camadas remota de capacidade FabricPool (nuvem) usando o ONTAP S3, configure LIFs entre clusters. Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- A política de serviço LIF já deve existir.

Sobre esta tarefa

Os LIFs não são necessários para a disposição em camadas do pool de malha local ou para servir aplicações S3 externas.

Passos

1. Liste as portas no cluster:

   `network port show`

   O exemplo a seguir mostra as portas de rede no `cluster01`:

   ```
   cluster01::> network port show
                                                                 Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Criar LIFs entre clusters no sistema:

   `network interface create -vserver Cluster -lif *LIF_name* -service-policy default-intercluster -home-node *node* -home-port *port* -address *port_IP* -netmask *netmask*`

   O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

   `network interface show –service-policy default-intercluster -failover`

   O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` na `e0c` porta irão falhar para a `e0d` porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Crie o servidor de armazenamento de objetos ONTAP S3

O servidor de armazenamento de objetos ONTAP gerencia dados como objetos S3, em vez de armazenamento de arquivos ou blocos fornecido pelos servidores ONTAP nas e SAN.

Antes de começar

Você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN não deve começar com um nome de intervalo. Ao acessar buckets usando o estilo virtual hospedado, o nome do servidor será usado como `mydomain.com`. Por exemplo, `bucketname.mydomain.com`.

Você deve ter um certificado de CA autoassinado (criado em etapas anteriores) ou um certificado assinado por um fornecedor de CA externo. Um certificado de CA não é necessário para um caso de uso local de disposição em camadas, em que o tráfego IP está passando apenas pelas LIFs de cluster.

Sobre esta tarefa

Quando um servidor de armazenamento de objetos é criado, um usuário raiz com UID 0 é criado. Nenhuma chave de acesso ou chave secreta é gerada para este usuário raiz. O administrador do ONTAP deve executar o `object-store-server users regenerate-keys` comando para definir a chave de acesso e a chave secreta para esse usuário.

> Como uma prática recomendada do NetApp, não use esse usuário root. Qualquer aplicativo cliente que use a chave de acesso ou chave secreta do usuário raiz tem acesso total a todos os buckets e objetos no armazenamento de objetos.

Consulte as `vserver object-store-server` páginas de manual para obter opções adicionais de configuração e exibição.

Exemplo 21. Passos

System Manager

Use este procedimento se estiver adicionando um servidor S3 a uma VM de armazenamento existente. Para adicionar um servidor S3 a uma nova VM de armazenamento, "Criar um SVM de storage em S3"consulte .

Você deve estar preparado para inserir endereços IP para dados de função de interface.

1. Habilite o S3 em uma VM de storage existente.
   a. Selecione a VM de armazenamento: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento, clique em **Settings** e, em seguida, clique em **S3**.
   b. Clique em **Ativar S3** e, em seguida, introduza o nome do servidor S3.
   c. Selecione o tipo de certificado.

      Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.

   d. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Crie o servidor S3:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   Você pode especificar opções adicionais ao criar o servidor S3 ou a qualquer momento mais tarde.

   - Se você estiver configurando a disposição em categorias locais, o nome do SVM pode ser um nome de data SVM ou SVM do sistema (cluster).
   - O nome do certificado deve ser o nome do certificado do servidor (usuário final ou certificado de folha) e não o certificado de CA do servidor (certificado de CA intermediário ou raiz).
   - O HTTPS é ativado por padrão na porta 443. Pode alterar o número da porta com a `-secure -listener-port` opção.

     Quando o HTTPS está ativado, os certificados de CA são necessários para a integração correta com SSL/TLS. A partir do ONTAP 9.15,1, o TLS 1,3 é compatível com armazenamento de objetos S3.

   - O HTTP está desativado por padrão. Quando ativado, o servidor escuta na porta 80. Você pode ativá-lo com a `-is-http-enabled` opção ou alterar o número da porta com a `-listener -port` opção.

Quando o HTTP está ativado, a solicitação e as respostas são enviadas pela rede em texto não criptografado.

2. Verifique se o S3 está configurado:

```
vserver object-store-server show
```

Exemplo

Este comando verifica os valores de configuração de todos os servidores de armazenamento de objetos:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Adicionar capacidade de storage a um SVM habilitado para S3

Crie um bucket do ONTAP S3

S3 objetos são mantidos em *buckets*. Eles não são aninhados como arquivos dentro de um diretório dentro de outros diretórios.

Antes de começar

Uma VM de armazenamento contendo um servidor S3 já deve existir.

Sobre esta tarefa

- A partir do ONTAP 9.14,1, o redimensionamento automático foi ativado em volumes FlexGroup S3 quando os intervalos são criados neles. Isso elimina a alocação excessiva de capacidade durante a criação do bucket em volumes FlexGroup novos e existentes. Os volumes FlexGroup são redimensionados para um tamanho mínimo necessário com base nas diretrizes a seguir. O tamanho mínimo necessário é o tamanho total de todos os buckets do S3 em um volume FlexGroup.
  - A partir do ONTAP 9.14,1, se um volume S3 FlexGroup for criado como parte de uma nova criação de bucket, o volume FlexGroup será criado com o tamanho mínimo necessário.
  - Se um volume S3 FlexGroup foi criado antes do ONTAP 9.14,1, o primeiro bucket criado ou excluído após o ONTAP 9.14,1 redimensiona o volume FlexGroup para o tamanho mínimo necessário.
  - Se um volume S3 FlexGroup foi criado antes do ONTAP 9.14,1 e já tinha o tamanho mínimo necessário, a criação ou eliminação de um bucket subsequente ao ONTAP 9.14,1 mantém o tamanho do volume S3 FlexGroup.

- Os níveis de serviço de storage são grupos de políticas de qualidade do serviço (QoS) adaptáveis predefinidos, com níveis padrão *value*, *performance* e *extreme*. Em vez de um dos níveis de serviço de storage padrão, você também pode definir um grupo de políticas de QoS personalizadas e aplicá-lo a um bucket. Para obter mais informações sobre definições de serviço de armazenamento, "Definições do serviço de armazenamento"consulte . Para obter mais informações sobre gerenciamento de desempenho, "Gerenciamento de desempenho"consulte . A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.
- Se você estiver configurando a disposição em camadas de capacidade local, crie buckets e usuários em uma VM de storage de dados, não na VM de storage do sistema onde o servidor S3 está localizado.
- Para acesso remoto ao cliente, você deve configurar buckets em uma VM de storage habilitada para S3. Se você criar um bucket em uma VM de storage que não esteja habilitada para S3, ele estará disponível somente para a disposição em categorias locais.
- Começando com ONTAP 9.14,1, você pode "Crie um bucket em um agregado espelhado ou sem espelhamento em uma configuração do MetroCluster".
- Para a CLI, quando você cria um bucket, você tem duas opções de provisionamento:
  - Deixe ONTAP Select os agregados subjacentes e componentes FlexGroup (padrão)
    - O ONTAP cria e configura um volume FlexGroup para o primeiro bucket selecionando automaticamente os agregados. Ele selecionará automaticamente o nível de serviço mais alto disponível para sua plataforma ou você pode especificar o nível de serviço de storage. Quaisquer buckets adicionais adicionados posteriormente à VM de storage terão o mesmo volume FlexGroup subjacente.
    - Como alternativa, você pode especificar se o bucket será usado para disposição em camadas, caso em que o ONTAP tenta selecionar Mídia de baixo custo com desempenho ideal para os dados em camadas.
  - Você seleciona os agregados subjacentes e componentes FlexGroup (requer opções de comando de privilégios avançados): Você tem a opção de selecionar manualmente os agregados nos quais o bucket e o volume FlexGroup contendo devem ser criados e, em seguida, especificar o número de constituintes em cada agregado. Ao adicionar baldes adicionais:
    - Se você especificar agregados e componentes para um novo bucket, um novo FlexGroup será criado para o novo bucket.
    - Se você não especificar agregados e componentes para um novo bucket, o novo bucket será adicionado a um FlexGroup existente. Consulte Gerenciamento de volumes do FlexGroup para obter mais informações.

      Quando você especifica agregados e constituintes ao criar um bucket, nenhum grupo de política de QoS, padrão ou personalizado, é aplicado. Você pode fazê-lo mais tarde com o `vserver object-store-server bucket modify` comando.

    Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-object-store-server-show.html[`vserver object-store-server bucket modify` em referência de comando ONTAP.

Observação: se você estiver servindo buckets do Cloud Volumes ONTAP, você deve usar o procedimento CLI. É altamente recomendável que você selecione manualmente os agregados subjacentes para garantir que eles estejam usando apenas um nó. O uso de agregados de ambos os nós pode afetar o desempenho, porque os nós estarão em zonas de disponibilidade geograficamente separadas e, portanto, suscetíveis a problemas de latência.

Crie buckets do S3 com a CLI do ONTAP

1. Se você pretende selecionar agregados e componentes do FlexGroup você mesmo, defina o nível de privilégio como avançado (caso contrário, o nível de privilégio de administrador é suficiente): `set -privilege advanced`
2. Criar um bucket:

   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

   O nome da VM de storage pode ser uma VM de storage de dados ou `Cluster` (o nome da VM de storage do sistema) se você estiver configurando a disposição em camadas local.

   Se você não especificar nenhuma opção, o ONTAP criará um bucket do 800GB com o nível de serviço definido para o nível mais alto disponível para o sistema.

   Se você quiser que o ONTAP crie um bucket com base no desempenho ou no uso, use uma das seguintes opções:

   - nível de serviço

     Inclua a `-storage-service-level` opção com um dos seguintes valores: `value`, `performance`, Ou `extreme`.

   - disposição em camadas

     Inclua a `-used-as-capacity-tier true` opção.

     Se você quiser especificar os agregados nos quais criar o volume FlexGroup subjacente, use as seguintes opções:

   - O `-aggr-list` parâmetro especifica a lista de agregados a serem usados para componentes de volume FlexGroup.

     Cada entrada na lista cria um constituinte no agregado especificado. Você pode especificar um agregado várias vezes para ter vários constituintes criados no agregado.

   Para obter performance consistente em todo o volume FlexGroup, todos os agregados precisam usar o mesmo tipo de disco e configurações de grupo RAID.

   - O `-aggr-list-multiplier` parâmetro especifica o número de vezes a iterar sobre os agregados que são listados com o `-aggr-list` parâmetro ao criar um volume FlexGroup.

     O valor padrão do `-aggr-list-multiplier` parâmetro é 4.

3. Adicione um grupo de políticas de QoS, se necessário:

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Verificar a criação do balde:

   `vserver object-store-server bucket show [-instance]`

Exemplo

O exemplo a seguir cria um bucket para a VM de armazenamento de `vs1` tamanho `1TB` e especificando o agregado:

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Crie buckets do S3 com o System Manager

1. Adicione um novo bucket em uma VM de storage habilitada para S3.
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.
      - Se você clicar em **Salvar** neste ponto, um bucket será criado com as seguintes configurações padrão:
        - Nenhum usuário tem acesso ao bucket, a menos que as políticas de grupo já estejam em vigor.

          Você não deve usar o usuário raiz do S3 para gerenciar o armazenamento de objetos do ONTAP e compartilhar suas permissões, pois ele tem acesso ilimitado ao armazenamento de objetos. Em vez disso, crie um usuário ou grupo com Privileges administrativo que você atribuir.

        - Um nível de qualidade de serviço (desempenho) que é o mais alto disponível para o seu sistema.
      - Clique em **Salvar** para criar um bucket com esses valores padrão.

Configurar permissões e restrições adicionais

Você pode clicar em **mais Opções** para configurar as configurações de bloqueio de objetos, permissões de usuário e nível de desempenho ao configurar o bucket, ou você pode modificar essas configurações posteriormente.

Se você pretende usar o armazenamento de objetos S3 para disposição em camadas do FabricPool, considere selecionar **usar para disposição em camadas** (usar Mídia de baixo custo com desempenho ideal para os dados em camadas) em vez de um nível de serviço de desempenho.

Se você quiser habilitar o controle de versão para seus objetos para recuperação posterior, selecione **Ativar controle de versão**. O controle de versão é habilitado por padrão se você estiver habilitando o bloqueio de objetos no bucket. Para obter informações sobre o controle de versão de objetos, consulte "Usando o controle de versão em buckets do S3 para Amazon".

A partir de 9.14.1, o bloqueio de objetos é suportado em buckets do S3. O bloqueio de objetos S3 requer uma licença SnapLock padrão. Esta licença está incluída no "ONTAP One". Antes do ONTAP One, a licença SnapLock foi incluída no pacote Segurança e conformidade. O pacote de segurança e conformidade já não é oferecido, mas ainda é válido. Embora não seja necessário atualmente, os clientes existentes podem optar por "Atualize para o ONTAP One". Se você estiver habilitando o bloqueio de objetos em um bucket, deverá "Verifique se uma licença SnapLock está instalada". Se uma licença do SnapLock não estiver instalada, você deve "instale" fazê-la antes de ativar o bloqueio de objetos. Quando tiver verificado que a licença SnapLock

está instalada, para proteger os objetos no bucket de serem excluídos ou substituídos, selecione **Ativar bloqueio de objetos**. O bloqueio pode ser ativado em todas as versões específicas de objetos e apenas quando o relógio SnapLock Compliance é inicializado para os nós de cluster. Siga estes passos:

1. Se o relógio SnapLock Compliance não for inicializado em nenhum nó do cluster, o botão **Inicializar Relógio SnapLock Compliance** será exibido. Clique em **Inicializar Relógio SnapLock Compliance** para inicializar o relógio SnapLock Compliance nos nós do cluster.
2. Selecione o modo **Governance** para ativar um bloqueio baseado em tempo que permite permissões *Write Once, Read many (WORM)* nos objetos. Mesmo no modo *Governance*, os objetos podem ser excluídos por usuários administradores com permissões específicas.
3. Selecione o modo **Compliance** se quiser atribuir regras mais rigorosas de exclusão e atualização nos objetos. Neste modo de bloqueio de objetos, os objetos podem ser expirados apenas na conclusão do período de retenção especificado. A menos que um período de retenção seja especificado, os objetos permanecem bloqueados indefinidamente.
4. Especifique o período de retenção para o bloqueio em dias ou anos se você quiser que o bloqueio seja efetivo por um determinado período.

> O bloqueio é aplicável a baldes S3 com controle de versão e sem controle de versão. O bloqueio de objetos não é aplicável a objetos nas.

Você pode configurar as configurações de proteção e permissão, bem como o nível de serviço de desempenho para o bucket.

> Você já deve ter criado usuários e grupos antes de configurar as permissões.

Para obter informações, "Criar espelho para um novo balde"consulte .

Verifique o acesso ao balde

Em aplicativos cliente S3 (seja ONTAP S3 ou um aplicativo externo de terceiros), você pode verificar seu acesso ao bucket recém-criado digitando o seguinte:

- O certificado da CA do servidor S3.
- A chave de acesso e a chave secreta do usuário.
- O nome do FQDN do servidor S3 e o nome do bucket.

Aumente ou diminua o tamanho do balde ONTAP S3

Quando necessário, você pode aumentar ou diminuir o tamanho de um balde existente.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para gerenciar o tamanho do bucket.

System Manager

1. Selecione **armazenamento > baldes** e localize o balde que pretende modificar.
2. Clique ⋮ ao lado do nome do intervalo e selecione **Editar**.
3. Na janela **Edit bucket**, altere a capacidade do bucket.
4. **Guardar**.

CLI

1. Alterar a capacidade do balde:

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

Crie um bucket do ONTAP S3 em um agregado espelhado ou sem espelhamento em uma configuração do MetroCluster

A partir do ONTAP 9.14,1, você pode provisionar um bucket em um agregado espelhado ou sem espelhamento nas configurações FC e IP do MetroCluster.

Sobre esta tarefa

- Por padrão, os buckets são provisionados em agregados espelhados.
- As mesmas diretrizes de provisionamento descritas em "Crie um bucket" aplicam-se à criação de um bucket em um ambiente MetroCluster.
- Os seguintes recursos de armazenamento de objetos S3 são **não** suportados em ambientes MetroCluster:
  - SnapMirror S3
  - Gerenciamento do ciclo de vida do bucket do S3
  - S3 bloqueio de objetos no modo **Compliance**

    ⓘ O bloqueio de objetos S3D no modo **Governance** é suportado.

  - Disposição em camadas no local FabricPool

Antes de começar

Um SVM que contenha um servidor S3 já deve existir.

Processo para criar buckets

CLI

1. Se você pretende selecionar agregados e componentes do FlexGroup você mesmo, defina o nível de privilégio como avançado (caso contrário, o nível de privilégio de administrador é suficiente): `set -privilege advanced`
2. Criar um bucket:

   `vserver object-store-server bucket create -vserver <svm_name> -bucket <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates true/false]`

   Defina a `-use-mirrored-aggregates` opção como `true` ou `false` dependendo se você deseja usar um agregado espelhado ou sem espelhamento.

   Por padrão, a `-use-mirrored-aggregates` opção é definida como `true`.

   - O nome do SVM deve ser um data SVM.
   - Se você não especificar nenhuma opção, o ONTAP criará um bucket do 800GB com o nível de serviço definido para o nível mais alto disponível para o sistema.
   - Se você quiser que o ONTAP crie um bucket com base no desempenho ou no uso, use uma das seguintes opções:
     - nível de serviço

       Inclua a `-storage-service-level` opção com um dos seguintes valores: `value`, `performance`, Ou `extreme`.

     - disposição em camadas

       Inclua a `-used-as-capacity-tier true` opção.
   - Se você quiser especificar os agregados nos quais criar o volume FlexGroup subjacente, use as seguintes opções:
     - O `-aggr-list` parâmetro especifica a lista de agregados a serem usados para componentes de volume FlexGroup.

       Cada entrada na lista cria um constituinte no agregado especificado. Você pode especificar um agregado várias vezes para ter vários constituintes criados no agregado.

   Para obter performance consistente em todo o volume FlexGroup, todos os agregados precisam usar o mesmo tipo de disco e configurações de grupo RAID.

   - O `-aggr-list-multiplier` parâmetro especifica o número de vezes a iterar sobre os agregados que são listados com o `-aggr-list` parâmetro ao criar um volume FlexGroup.

     O valor padrão do `-aggr-list-multiplier` parâmetro é 4.
3. Adicione um grupo de políticas de QoS, se necessário:

   `vserver object-store-server bucket modify -bucket *bucket_name* -qos-policy -group *qos_policy_group*`

4. Verificar a criação do balde:

```
vserver object-store-server bucket show [-instance]
```

Exemplo

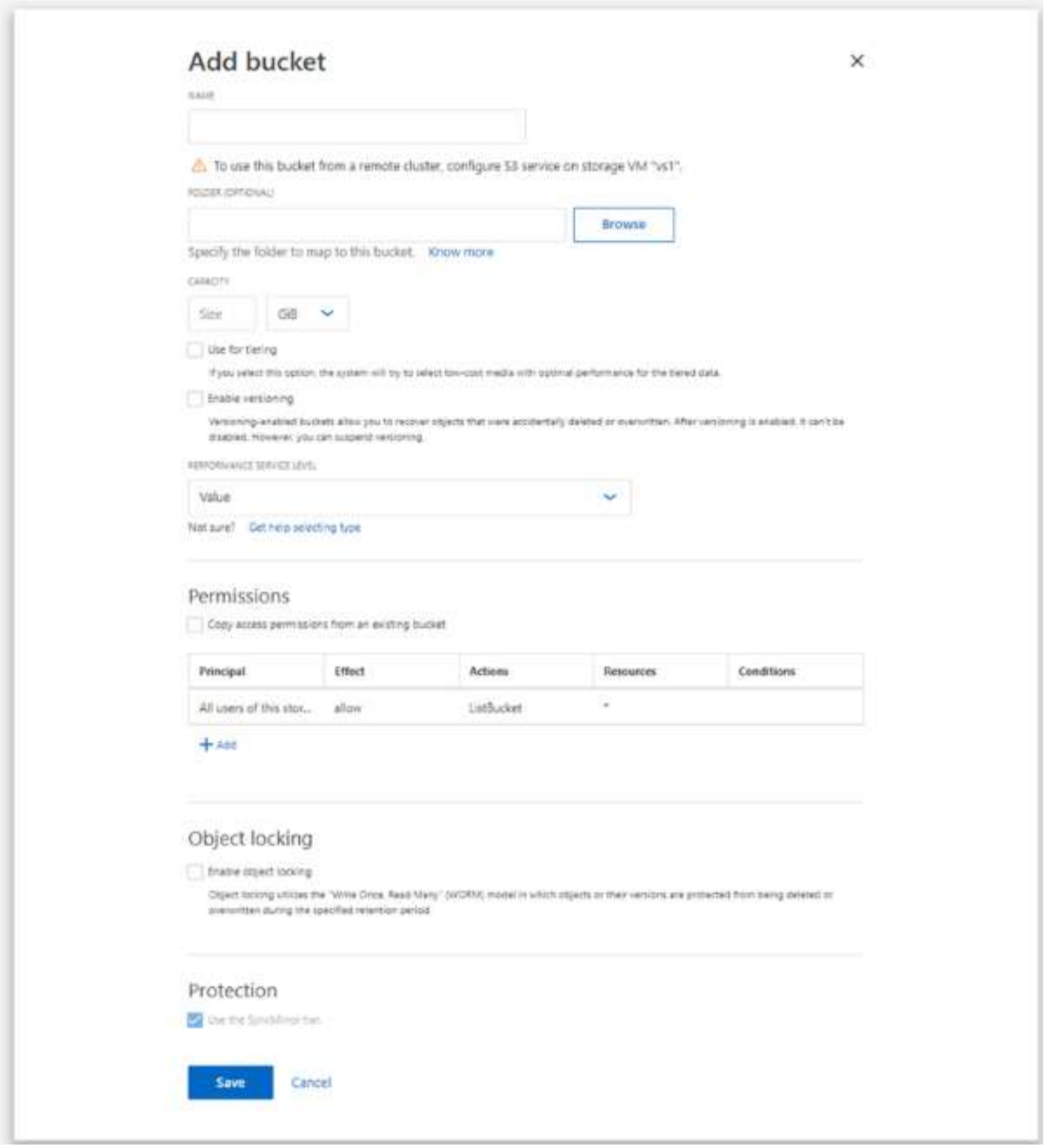
O exemplo a seguir cria um bucket do SVM VS1 de tamanho 1TB em um agregado espelhado:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Adicione um novo bucket em uma VM de storage habilitada para S3.
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Por padrão, o bucket é provisionado em um agregado espelhado. Se você quiser criar um bucket em um agregado sem espelhamento, selecione **mais opções** e desmarque a caixa **Use the SyncMirror Tier** sob **proteção** conforme mostrado na imagem a seguir:



- Se você clicar em **Salvar** neste ponto, um bucket será criado com as seguintes configurações padrão:
  - Nenhum usuário tem acesso ao bucket, a menos que as políticas de grupo já estejam em vigor.

> Você não deve usar o usuário raiz do S3 para gerenciar o armazenamento de objetos do ONTAP e compartilhar suas permissões, pois ele tem acesso ilimitado ao armazenamento de objetos. Em vez disso, crie um usuário ou grupo com Privileges administrativo que você atribuir.

  - Um nível de qualidade de serviço (desempenho) que é o mais alto disponível para o seu sistema.
- Você pode clicar em **mais Opções** para configurar permissões de usuário e nível de desempenho ao configurar o bucket, ou você pode modificar essas configurações

posteriormente.

- Você já deve ter criado usuários e grupos antes de usar **mais Opções** para configurar suas permissões.
- Se você pretende usar o armazenamento de objetos S3 para disposição em camadas do FabricPool, considere selecionar **usar para disposição em camadas** (usar Mídia de baixo custo com desempenho ideal para os dados em camadas) em vez de um nível de serviço de desempenho.

2. Em aplicativos cliente S3 (outro sistema ONTAP ou um aplicativo externo de 3rd parceiros), verifique o acesso ao novo bucket inserindo o seguinte:
   - O certificado da CA do servidor S3.
   - A chave de acesso e a chave secreta do usuário.
   - O nome do FQDN do servidor S3 e o nome do bucket.

Criar uma regra de gerenciamento do ciclo de vida do bucket do ONTAP S3

A partir do ONTAP 9.13,1, é possível criar regras de gerenciamento de ciclo de vida para gerenciar os ciclos de vida dos objetos nos buckets do S3. Você pode definir regras de exclusão para objetos específicos em um bucket e, por meio dessas regras, expirar esses objetos de bucket. Isso permite que você atenda aos requisitos de retenção e gerencie o storage geral de objetos do S3 com eficiência.

Se o bloqueio de objetos estiver ativado para os objetos de bucket, as regras de gerenciamento de ciclo de vida para expiração de objetos não serão aplicadas em objetos bloqueados. Para obter informações sobre o bloqueio de objetos, "Crie um bucket"consulte .

Antes de começar

- Um SVM habilitado para S3 que contenha um servidor S3 e um bucket já deve existir. Consulte "Criar um SVM para S3" para obter mais informações.
- Você deve estar ciente de que as regras de gerenciamento do ciclo de vida do bucket não são compatíveis com configurações do MetroCluster.

Sobre esta tarefa

Ao criar suas regras de gerenciamento de ciclo de vida, você pode aplicar as seguintes ações de exclusão aos objetos bucket:

- Exclusão de versões atuais - esta ação expira objetos identificados pela regra. Se o controle de versão estiver habilitado no bucket, o S3 tornará todos os objetos expirados indisponíveis. Se o controle de versão não estiver habilitado, essa regra excluirá os objetos permanentemente. A ação CLI é `Expiration`.
- Exclusão de versões não-atuais - esta ação especifica quando S3 pode remover permanentemente objetos não-atuais. A ação CLI é `NoncurrentVersionExpiration`.

Uma versão não atual é baseada no tempo de criação ou modificação da versão atual. A remoção atrasada de objetos não atuais pode ser útil quando você exclui ou sobrescreve acidentalmente um objeto. Por exemplo, você pode configurar uma regra de expiração para excluir versões não-atuais cinco dias após elas se tornarem não-atuais. Por exemplo, suponha que em 1/1/2014 às 10:30 UTC (horário de Brasília) você crie um objeto chamado `photo.gif` (ID da versão `111111`). Em 1/2/2014 às 11:30 UTC (horário de Brasília), você exclui acidentalmente `photo.gif` (ID da versão `111111`), o que cria um marcador de exclusão com um novo ID de versão (como ID da versão `4857693`). Agora você tem cinco dias para recuperar a versão original `photo.gif` do (ID da versão `111111`) antes que a exclusão seja permanente. Em 1/8/2014 às 00:00 UTC, a regra de ciclo de vida para expiração é executada e exclui permanentemente `photo.gif` (ID da versão `111111`), cinco dias depois que se tornou uma versão não atual.

- Eliminação de marcadores de eliminação expirados - esta ação elimina marcadores de eliminação de objetos expirados. Em buckets habilitados para versionamento, objetos com marcadores de exclusão se tornam as versões atuais dos objetos. Os objetos não são excluídos e nenhuma ação pode ser executada neles. Esses objetos expiram quando não há versões atuais associadas a eles. A ação CLI é `Expiration`.
- Eliminação de carregamentos de várias partes incompletos - esta ação define um tempo máximo (em dias) que pretende permitir que os carregamentos de várias partes permaneçam em curso. Depois disso, eles são excluídos. A ação CLI é `AbortIncompleteMultipartUpload`.

O procedimento que você segue depende da interface que você usa. Com o ONTAP 9.13,1, você precisa usar o CLI. A partir do ONTAP 9.14,1, você também pode usar o Gerenciador do sistema.

Gerencie regras de gerenciamento de ciclo de vida com a CLI

A partir do ONTAP 9.13,1, você pode usar a CLI do ONTAP para criar regras de gerenciamento de ciclo de vida para expirar objetos nos buckets do S3.

Antes de começar

Para a CLI, você precisa definir os campos obrigatórios para cada tipo de ação de expiração ao criar uma regra de gerenciamento do ciclo de vida do bucket. Esses campos podem ser modificados após a criação inicial. A tabela a seguir exibe os campos exclusivos para cada tipo de ação.

Tipo de ação	Campos únicos
Não CurrentVersionExpiration	• `-non-curr-days` - Número de dias após os quais as versões não atuais serão excluídas • `-new-non-curr-versions` - Número de versões não atuais mais recentes a reter
Expiração	• `-obj-age-days` - Número de dias desde a criação, após o qual a versão atual dos objetos pode ser excluída • `-obj-exp-date` - Data específica em que os objetos devem expirar • `-expired-obj-del-markers` - Limpar marcadores de exclusão de objeto

AbortIncompleteMultipartUpload	• `-after-initiation-days` - Número de dias de início, após o qual o upload pode ser abortado

Para que a regra de gerenciamento do ciclo de vida do bucket seja aplicada somente a um subconjunto específico de objetos, os administradores devem definir cada filtro ao criar a regra. Se esses filtros não forem definidos ao criar a regra, a regra será aplicada a todos os objetos dentro do intervalo.

Todos os filtros podem ser modificados após a criação inicial *exceto* para o seguinte

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Passos

1. Use o `vserver object-store-server bucket lifecycle-management-rule create` comando com campos obrigatórios para o seu tipo de ação de expiração para criar a regra de gerenciamento do ciclo de vida do bucket.

Exemplo

O comando a seguir cria uma regra de gerenciamento do ciclo de vida do bucket NonCurrentVersionExpiration:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Exemplo

O comando a seguir cria uma regra de gerenciamento do ciclo de vida do bucket Expiration:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Exemplo

O comando a seguir cria uma regra de gerenciamento do ciclo de vida do bucket do

AbortIncompleteMultipartUpload:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Gerencie regras de gerenciamento de ciclo de vida com o System Manager

A partir do ONTAP 9.14,1, você pode expirar S3 objetos usando o Gerenciador de sistema. Você pode adicionar, editar e excluir regras de gerenciamento de ciclo de vida para seus objetos S3D. Além disso, você pode importar uma regra de ciclo de vida criada para um bucket e utilizá-la para os objetos em outro bucket. Você pode desativar uma regra ativa e ativá-la mais tarde.

Adicionar uma regra de gerenciamento de ciclo de vida

1. Clique em **armazenamento > baldes**.
2. Selecione o intervalo para o qual você deseja especificar a regra de expiração.
3. Clique no ⋮ ícone e selecione **Gerenciar regras de ciclo de vida**.
4. Clique em **Add > Lifecycle rule**.
5. Na página Adicionar uma regra de ciclo de vida, adicione o nome da regra.
6. Defina o escopo da regra, se você deseja que ela seja aplicada a todos os objetos no bucket ou em objetos específicos. Se você quiser especificar objetos, adicione pelo menos um dos seguintes critérios de filtro:
   a. Prefixo: Especifique um prefixo dos nomes das chaves do objeto aos quais a regra deve ser aplicada. Normalmente, é o caminho ou pasta do objeto. Você pode inserir um prefixo por regra. A menos que um prefixo válido seja fornecido, a regra se aplica a todos os objetos em um bucket.
   b. Tags: Especifique até três pares de chaves e valores (tags) para os objetos aos quais a regra deve ser aplicada. Somente chaves válidas são usadas para filtragem. O valor é opcional. No entanto, se você adicionar valores, certifique-se de adicionar apenas valores válidos para as chaves correspondentes.
   c. Tamanho: Você pode limitar o escopo entre os tamanhos mínimo e máximo dos objetos. Pode introduzir um ou ambos os valores. A unidade padrão é MIB.
7. Especifique a ação:
   a. **Expire a versão atual dos objetos**: Defina uma regra para tornar todos os objetos atuais permanentemente indisponíveis após um número específico de dias desde a sua criação ou em uma data específica. Esta opção não estará disponível se a opção **Excluir marcadores de exclusão de objetos expirados** estiver selecionada.
   b. **Excluir permanentemente versões não atuais**: Especifique o número de dias após os quais a versão não atual é excluída e o número de versões a serem mantidas.
   c. **Excluir marcadores de exclusão de objetos expirados**: Selecione esta ação para excluir objetos com marcadores de exclusão expirados, ou seja, excluir marcadores sem um objeto atual associado.

Essa opção fica indisponível quando você seleciona a opção **expire a versão atual dos objetos** que exclui automaticamente todos os objetos após o período de retenção. Essa opção também fica indisponível quando tags de objeto são usadas para filtragem.

d. **Excluir carregamentos de várias partes incompletos**: Defina o número de dias após os quais os uploads de várias partes incompletos serão excluídos. Se os uploads de várias partes que estão em andamento falharem dentro do período de retenção especificado, você poderá excluir os uploads de várias partes incompletos. Esta opção fica indisponível quando as tags de objeto são usadas para filtragem.

e. Clique em **Salvar**.

Importar uma regra de ciclo de vida

1. Clique em **armazenamento > baldes**.
2. Selecione o intervalo para o qual você deseja importar a regra de expiração.
3. Clique no ⋮ ícone e selecione **Gerenciar regras de ciclo de vida**.
4. Clique em **Adicionar > Importar uma regra**.
5. Selecione o intervalo a partir do qual você deseja importar a regra. As regras de gerenciamento de ciclo de vida definidas para o bucket selecionado são exibidas.
6. Selecione a regra que pretende importar. Você tem a opção de selecionar uma regra de cada vez, sendo a seleção padrão a primeira regra.
7. Clique em **Importar**.

Edite, exclua ou desative uma regra

Você só pode editar as ações de gerenciamento de ciclo de vida associadas à regra. Se a regra foi filtrada com tags de objeto, as opções **Excluir marcadores de exclusão de objeto expirados** e **Excluir carregamentos de várias partes incompletos** não estarão disponíveis.

Quando você exclui uma regra, essa regra não se aplicará mais a objetos associados anteriormente.

1. Clique em **armazenamento > baldes**.
2. Selecione o intervalo para o qual deseja editar, excluir ou desativar a regra de gerenciamento de ciclo de vida.
3. Clique no ⋮ ícone e selecione **Gerenciar regras de ciclo de vida**.
4. Selecione a regra pretendida. Você pode editar e desativar uma regra de cada vez. Você pode excluir várias regras de uma só vez.
5. Selecione **Edit**, **Delete** ou **Disable** e conclua o procedimento.

Crie um usuário do ONTAP S3

Crie um usuário S3 com permissões específicas. A autorização do usuário é necessária em todos os armazenamentos de objetos ONTAP para restringir a conetividade a clientes autorizados.

Antes de começar.

Uma VM de storage habilitada para S3 já deve existir.

Sobre esta tarefa

Um usuário S3 pode ter acesso a qualquer bucket em uma VM de armazenamento. Quando você cria um usuário S3, uma chave de acesso e uma chave secreta também são gerados para o usuário. Eles devem ser compartilhados com o usuário juntamente com o FQDN do armazenamento de objetos e o nome do bucket.

Para maior segurança, a partir de ONTAP 9.15,1, as chaves de acesso e as chaves secretas só são exibidas no momento em que o usuário S3 é criado e não podem ser exibidas novamente. Se as chaves forem perdidas, "novas chaves devem ser regeneradas".

Você pode conceder permissões de acesso específicas a usuários do S3 em uma política de bucket ou uma diretiva de servidor de objetos.

Quando você cria um novo servidor de armazenamento de objetos, o ONTAP cria um usuário raiz (UID 0), que é um usuário privilegiado com acesso a todos os buckets. Em vez de administrar o ONTAP S3 como usuário raiz, o NetApp recomenda que uma função de usuário de administrador seja criada com Privileges específicos.

CLI

1. Criar um usuário S3:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - Adicionar um comentário é opcional.
   - A partir de ONTAP 9.14,1, pode definir o período de tempo para o qual a chave será válida no `-key-time-to-live` parâmetro. Você pode adicionar o período de retenção neste formato para indicar o período após o qual a chave de acesso expira: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Por exemplo, se você quiser inserir um período de retenção de um dia, duas horas, três minutos e quatro segundos, digite o valor como `P1DT2H3M4S`. A menos que especificado, a chave é válida por um período de tempo indefinido.

     O exemplo abaixo cria um usuário com nome `sm_user1` na VM de armazenamento `vs0` , com um período de retenção de chave de uma semana.

```
vserver object-store-server user create -vserver vs0 -user sm_user1
-key-time-to-live P1W
```

2. Certifique-se de salvar a chave de acesso e a chave secreta. Eles serão necessários para acesso de clientes S3.

System Manager

1. Clique em **Storage > Storage VMs**. Selecione a VM de armazenamento à qual você precisa adicionar um usuário, selecione **Configurações** e clique em S3.
2. Para adicionar um usuário, clique em **usuários > Adicionar**.
3. Introduza um nome para o utilizador.
4. A partir do ONTAP 9.14,1, você pode especificar o período de retenção das chaves de acesso que são criadas para o usuário. Você pode especificar o período de retenção em dias, horas, minutos ou segundos, após o qual as chaves expiram automaticamente. Por padrão, o valor é definido como `0` que indica que a chave é válida indefinidamente.
5. Clique em **Salvar**. O usuário é criado e uma chave de acesso e uma chave secreta são geradas para o usuário.
6. Transfira ou guarde a chave de acesso e a chave secreta. Eles serão necessários para acesso de clientes S3.

Próximas etapas

- Criar ou modificar grupos S3

Crie ou modifique grupos de usuários do ONTAP S3 para controlar o acesso aos buckets

Você pode simplificar o acesso ao bucket criando grupos de usuários com autorizações de acesso apropriadas.

Antes de começar

S3 usuários em um SVM habilitado para S3 já devem existir.

Sobre esta tarefa

Os usuários de um grupo S3 podem ter acesso a qualquer bucket em um SVM, mas não em vários SVMs. As permissões de acesso de grupo podem ser configuradas de duas maneiras:

- Ao nível do balde

  Depois de criar um grupo de usuários do S3, você especifica permissões de grupo em declarações de política de bucket e elas se aplicam somente a esse bucket.

- No nível da SVM

  Depois de criar um grupo de usuários S3, você especifica nomes de diretiva de servidor de objetos na definição de grupo. Essas políticas determinam os buckets e o acesso dos membros do grupo.

System Manager

1. Edite a VM de armazenamento: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.
2. Adicionar um grupo: Selecione **grupos** e, em seguida, selecione **Adicionar**.
3. Introduza um nome de grupo e selecione a partir de uma lista de utilizadores.
4. Você pode selecionar uma política de grupo existente ou adicionar uma agora, ou pode adicionar uma política mais tarde.

CLI

1. Criar um grupo S3:
   `vserver object-store-server group create -vserver` *`svm_name`* `-name` *`group_name`* `-users` *`user_name\(s\)`* `[-policies` *`policy_names`*`] [-comment` *`text`*`\]` A `-policies` opção pode ser omitida em configurações com apenas um bucket em um armazenamento de objetos; o nome do grupo pode ser adicionado à política de bucket. A `-policies` opção pode ser adicionada mais tarde com o `vserver object-store-server group modify` comando após a criação de políticas de servidor de armazenamento de objetos.

Regenere as chaves ONTAP S3 e modifique seu período de retenção

Chaves de acesso e chaves secretas são geradas automaticamente durante a criação do usuário para habilitar o acesso do cliente S3. Você pode regenerar chaves para um usuário se uma chave estiver expirada ou comprometida.

Para obter informações sobre a geração de chaves de acesso, "Crie um usuário S3"consulte .

System Manager

1. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
2. Na guia **Settings**, clique no mosaico **S3**.
3. Na guia **usuários**, verifique se não há nenhuma chave de acesso ou se a chave expirou para o usuário.
4. Se você precisar regenerar a chave, clique ao lado do usuário e clique em **regenerar chave**.
5. Por padrão, as chaves geradas são válidas por um período de tempo indefinido. A partir de 9.14.1, você pode modificar seu período de retenção, após o qual as chaves expiram automaticamente. Insira o período de retenção em dias, horas, minutos ou segundos.
6. Clique em **Salvar**. A chave é regenerada. Qualquer alteração no período de retenção da chave entra em vigor imediatamente.
7. Transfira ou guarde a chave de acesso e a chave secreta. Eles serão necessários para acesso de clientes S3.

CLI

1. Regenere o acesso e as chaves secretas para um usuário executando o `vserver object-store-server user regenerate-keys` comando.
2. Por padrão, as chaves geradas são válidas indefinidamente. A partir de 9.14.1, você pode modificar seu período de retenção, após o qual as chaves expiram automaticamente. Você pode adicionar o período de retenção neste formato: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Por exemplo, se quiser inserir um período de retenção de um dia, duas horas, três minutos e quatro segundos, digite o valor como `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. Guarde as chaves de acesso e secretas. Eles serão necessários para acesso de clientes S3.

Criar ou modificar instruções de política de acesso

Saiba mais sobre as políticas de servidor de armazenamento de objetos e bucket do ONTAP S3

O acesso de usuário e grupo a recursos do S3 é controlado por políticas de servidor de armazenamento de objetos e bucket. Se você tem um pequeno número de usuários ou grupos, controlar o acesso no nível do bucket provavelmente é suficiente, mas se você tiver muitos usuários e grupos, é mais fácil controlar o acesso no nível do servidor do armazenamento de objetos.

Adicione regras de acesso à política de bucket do ONTAP S3 padrão

Você pode adicionar regras de acesso à política de bucket padrão. O escopo de seu controle de acesso é o balde contendo, portanto, é mais apropriado quando há um único balde.

Antes de começar

Uma VM de armazenamento habilitada para S3 contendo um servidor S3 e um bucket já deve existir.

Você já deve ter criado usuários ou grupos antes de conceder permissões.

Sobre esta tarefa

Você pode adicionar novas instruções para novos usuários e grupos ou modificar os atributos de instruções existentes. Para obter mais opções, consulte as `vserver object-store-server bucket policy` páginas de manual.

Permissões de usuário e grupo podem ser concedidas quando o bucket é criado ou conforme necessário mais tarde. Você também pode modificar a capacidade do bucket e a atribuição do grupo de políticas de QoS.

A partir do ONTAP 9.9,1, se você planeja oferecer suporte à funcionalidade de marcação de objetos cliente AWS com o servidor ONTAP S3, as ações `GetObjectTagging` `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Passos

1. Edite o bucket: Clique em **Storage > Buckets**, clique no bucket desejado e clique em **Edit**. Ao adicionar ou modificar permissões, você pode especificar os seguintes parâmetros:
   - **Principal**: O usuário ou grupo a quem o acesso é concedido.
   - **Efeito**: Permite ou nega o acesso a um usuário ou grupo.
   - **Ações**: Ações permitidas no intervalo para um determinado usuário ou grupo.
   - **Recursos**: Caminhos e nomes de objetos dentro do intervalo para o qual o acesso é concedido ou negado.

     Os padrões ***bucketname*** e ***bucketname/**** concedem acesso a todos os objetos no bucket. Você também pode conceder acesso a objetos únicos; por exemplo, ***bucketname/*_readme.txt**.

   - **Condições** (opcional): Expressões que são avaliadas quando o acesso é tentado. Por exemplo, você pode especificar uma lista de endereços IP para os quais o acesso será permitido ou negado.

> A partir do ONTAP 9.14,1, você pode especificar variáveis para a política de bucket no campo **Resources**. Essas variáveis são marcadores de posição que são substituídos por valores contextuais quando a política é avaliada. Por exemplo, se `${aws:username}` for especificado como uma variável para uma política, essa variável será substituída pelo nome de usuário do contexto de solicitação e a ação da política pode ser executada como configurada para esse usuário.

CLI

Passos

1. Adicione uma instrução a uma política de bucket:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   Os seguintes parâmetros definem permissões de acesso:

`-effect`	A declaração pode permitir ou negar acesso
`-action`	Você pode especificar `*` para indicar todas as ações ou uma lista de uma ou mais das seguintes opções: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, E `ListMultipartUploadParts`.

`-principal`	Uma lista de um ou mais S3 usuários ou grupos. • Um máximo de 10 usuários ou grupos podem ser especificados. • Se um grupo S3 for especificado, ele deverá estar no formulário `group/group_name`. • `*` pode ser especificado para significar acesso público; ou seja, acesso sem uma chave de acesso e chave secreta. • Se nenhum principal for especificado, todos os usuários do S3 na VM de armazenamento terão acesso.
`-resource`	O balde e qualquer objeto que ele contém. Os carateres curinga `*` e `?` podem ser usados para formar uma expressão regular para especificar um recurso. Para um recurso, você pode especificar variáveis em uma política. Estas são variáveis de política são marcadores de posição que são substituídos pelos valores contextuais quando a política é avaliada.

Opcionalmente, você pode especificar uma cadeia de texto como comentário com a `-sid` opção.

Exemplos

O exemplo a seguir cria uma declaração de política de bucket do servidor de armazenamento de objetos para a VM de armazenamento svm1.example.com e bucket1 que especifica o acesso permitido a uma pasta readme para o usuário do servidor de armazenamento de objetos user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

O exemplo a seguir cria uma declaração de política de bucket do servidor de armazenamento de objetos para a VM de armazenamento svm1.example.com e bucket1 que especifica o acesso permitido a todos os objetos para o grupo de servidores de armazenamento de objetos group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partir do ONTAP 9.14,1, você pode especificar variáveis para uma política de bucket. O exemplo a seguir cria uma declaração de política de bucket do servidor para a VM de armazenamento `svm1` e `bucket1` especifica `${aws:username}` como uma variável para um recurso de diretiva. Quando a política é avaliada, a variável de política é substituída pelo nome de usuário de contexto de solicitação e a ação de política pode ser executada como configurada para esse usuário. Por exemplo, quando a seguinte declaração de política é avaliada, `${aws:username}` é substituída pelo usuário que executa a operação S3. Se um usuário `user1` executar a operação, esse usuário terá acesso ao `bucket1` as `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Criar ou modificar uma política de servidor de armazenamento de objetos ONTAP S3

Você pode criar políticas que podem ser aplicadas a um ou mais buckets em um armazenamento de objetos. As políticas de servidor de armazenamento de objetos podem ser anexadas a grupos de usuários, simplificando assim o gerenciamento do acesso a recursos em vários buckets.

Antes de começar

Um SVM habilitado para S3 que contenha um servidor S3 e um bucket já deve existir.

Sobre esta tarefa

É possível habilitar políticas de acesso no nível SVM especificando uma política padrão ou personalizada em um grupo de servidores de storage de objetos. As políticas não entram em vigor até que sejam especificadas na definição de grupo.

> Quando você usa políticas de servidor de armazenamento de objetos, você especifica princípios (ou seja, usuários e grupos) na definição de grupo, não na própria política.

Há três políticas padrão somente leitura para acesso aos recursos do ONTAP S3:

- FullAccess
- NoS3Access
- ReadOnlyAccess

Você também pode criar novas políticas personalizadas, adicionar novas instruções para novos usuários e grupos ou modificar os atributos de instruções existentes. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/index.html[`vserver object-store-server policy` em referência de comando ONTAP.

A partir do ONTAP 9.9,1, se você planeja oferecer suporte à funcionalidade de marcação de objetos cliente AWS com o servidor ONTAP S3, as ações `GetObjectTagging` `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar ou modificar uma política de servidor de armazenamento de objetos

Passos

1. Edite a VM de armazenamento: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.
2. Adicionar um usuário: Clique em **políticas** e, em seguida, clique em **Adicionar**.
   a. Introduza um nome de política e selecione a partir de uma lista de grupos.
   b. Selecione uma política padrão existente ou adicione uma nova.

      Ao adicionar ou modificar uma política de grupo, você pode especificar os seguintes parâmetros:

      - Grupo: Os grupos a quem o acesso é concedido.
      - Efeito: Permite ou nega o acesso a um ou mais grupos.
      - Ações: Ações permitidas em um ou mais buckets para um determinado grupo.
      - Recursos: Caminhos e nomes de objetos dentro de um ou mais buckets para os quais o acesso é concedido ou negado. Por exemplo:
        - ***** Concede acesso a todos os buckets na VM de armazenamento.
        - **bucketname** e **bucketname/*** concedem acesso a todos os objetos em um bucket específico.
        - **bucketname/readme.txt** concede acesso a um objeto em um intervalo específico.
   c. Se desejar, adicione instruções às políticas existentes.

CLI

Use a CLI para criar ou modificar uma política de servidor de armazenamento de objetos

Passos

1. Criar uma política de servidor de armazenamento de objetos:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Crie uma declaração para a política:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Os seguintes parâmetros definem permissões de acesso:

`-effect`	A declaração pode permitir ou negar acesso

`-action`	Você pode especificar `*` para indicar todas as ações ou uma lista de uma ou mais das seguintes opções: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, E `ListMultipartUploadParts`.
`-resource`	O balde e qualquer objeto que ele contém. Os carateres curinga `*` e `?` podem ser usados para formar uma expressão regular para especificar um recurso.

Opcionalmente, você pode especificar uma cadeia de texto como comentário com a `-sid` opção.

Por padrão, novas instruções são adicionadas ao final da lista de instruções, que são processadas em ordem. Quando você adiciona ou modifica instruções mais tarde, você tem a opção de modificar a configuração da instrução `-index` para alterar a ordem de processamento.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Configurar serviços de diretório externo para acesso ao ONTAP S3

A partir do ONTAP 9.14,1, os serviços para diretórios externos foram integrados ao armazenamento de objetos ONTAP S3. Essa integração simplifica o gerenciamento de usuários e acessos por meio de serviços de diretório externos.

Você pode fornecer grupos de usuários pertencentes a um serviço de diretório externo com acesso ao ambiente de storage de objetos do ONTAP. O LDAP (Lightweight Directory Access Protocol) é uma interface para comunicação com serviços de diretório, como o ative Directory, que fornece um banco de dados e serviços para gerenciamento de identidade e acesso (IAM). Para fornecer acesso, é necessário configurar grupos LDAP no ambiente do ONTAP S3. Depois de configurar o acesso, os membros do grupo têm permissões para buckets do ONTAP S3. Para obter informações sobre LDAP, "Visão geral do uso do LDAP"consulte .

Você também pode configurar grupos de usuários do ative Directory para o modo de vinculação rápida, para que as credenciais de usuário possam ser validadas e aplicativos S3 de terceiros e de código aberto possam ser autenticados por conexões LDAP.

Antes de começar

Antes de configurar grupos LDAP e ativar o modo de ligação rápida para acesso a grupos, certifique-se de que o seguinte é:

1. Uma VM de armazenamento habilitada para S3 contendo um servidor S3 foi criada. "Criar um SVM para S3"Consulte .
2. Um bucket foi criado nessa VM de storage. "Crie um bucket"Consulte .
3. O DNS está configurado na VM de armazenamento. "Configurar serviços DNS"Consulte .

4. Um certificado de autoridade de certificação raiz (CA) autoassinado do servidor LDAP é instalado na VM de armazenamento. "Instale o certificado de CA raiz autoassinado no SVM"Consulte .
5. Um cliente LDAP é configurado com TLS habilitado no SVM. "Crie uma configuração de cliente LDAP"Consulte e "Associe a configuração do cliente LDAP a SVMs para obter informações".

Configurar o acesso S3 para serviços de diretório externo

1. Especifique LDAP como o banco de dados *name Service* do SVM para o grupo e a senha para LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Crie uma declaração de política de bucket do armazenamento de objetos com o `principal` conjunto para o grupo LDAP ao qual você deseja conceder acesso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Exemplo: O exemplo a seguir cria uma declaração de política de bucket para `buck1`. A política permite o acesso do grupo LDAP `group1` ao recurso (bucket e seus objetos `buck1`) .

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verifique se um usuário do grupo LDAP `group1` é capaz de executar operações S3 do cliente S3.

Use o modo LDAP fast bind para autenticação

1. Especifique LDAP como o banco de dados *name Service* do SVM para o grupo e a senha para LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Certifique-se de que um usuário LDAP acessando o bucket do S3 tenha permissões definidas nas políticas de bucket. Para obter mais informações, "Modificar uma política de bucket"consulte .
3. Verifique se um usuário do grupo LDAP pode executar as seguintes operações:
   a. Configure a chave de acesso no cliente S3 neste formato: `"NTAPFASTBIND" + base64-encode(user-name:password)` Exemplo `"NTAPFASTBIND"`: base64-encode(ldapuser:password), o que resulta em `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      O cliente S3 pode pedir uma chave secreta. Na ausência de uma chave secreta, qualquer senha de pelo menos 16 carateres pode ser inserida.

   b. Execute operações S3 básicas do cliente S3 para o qual o usuário tem permissões.

Autenticação de recursos para o ative Directory para usuários sem UID e GID

Se o nasgroup especificado na declaração bucket-policy ou os usuários que fazem parte do nasgroup não tiverem UID e GID definidos, as pesquisas falharão quando esses atributos não forem encontrados.

Para evitar falhas de pesquisa, o NetApp recomenda o uso de domínios confiáveis para autorização de recursos no formato UPN: Nasgroup/group@trusted_domain.com

Para gerar as chaves de acesso do usuário para usuários de domínio confiáveis quando o LDAP fast bind não é usado

Use o `s3/services/<svm_uuid>/users` endpoint com usuários especificados no formato UPN. Exemplo:

```
$curl -siku FQDN\\user:<user_name> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn](https://github.com/fqdn)>,"<key_time_to_live>":"PT6H3M
"}'
```

Habilite os usuários LDAP ou de domínio para gerar suas próprias chaves de acesso ONTAP S3

A partir do ONTAP 9.14,1, como administrador do ONTAP, você pode criar funções personalizadas e concedê-las a grupos locais ou de domínio ou a grupos LDAP (Lightweight Directory Access Protocol), de modo que os usuários pertencentes a esses grupos possam gerar seu próprio acesso e chaves secretas para acesso ao cliente S3.

Você precisa executar algumas etapas de configuração em sua VM de armazenamento, para que a função personalizada possa ser criada e atribuída ao usuário que invoca a API para geração de chaves de acesso.

Antes de começar

Certifique-se de que:

1. Uma VM de armazenamento habilitada para S3 contendo um servidor S3 foi criada. "Criar um SVM para S3"Consulte .
2. Um bucket foi criado nessa VM de storage. "Crie um bucket"Consulte .
3. O DNS está configurado na VM de armazenamento. "Configurar serviços DNS"Consulte .
4. Um certificado de autoridade de certificação raiz (CA) autoassinado do servidor LDAP é instalado na VM de armazenamento. "Instale o certificado de CA raiz autoassinado no SVM"Consulte .
5. Um cliente LDAP é configurado com TLS ativado na VM de armazenamento. "Crie uma configuração de cliente LDAP"Consulte .
6. Associe a configuração do cliente ao SVM. "Associe a configuração do cliente LDAP a SVMs"Consulte . Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//vserver-services-name-service-ldap-create.html[`vserver services name-service ldap create`em referência de comando ONTAP.
7. Se você estiver usando uma VM de armazenamento de dados, crie uma interface de rede de gerenciamento (LIF) e na VM e também uma política de serviço para o LIF. Saiba mais sobre os[`network interface create`[`network interface service-policy create` comandos em ONTAP.

Configurar usuários para geração de chaves de acesso

1. Especifique LDAP como o banco de dados *name Service* da VM de armazenamento para o grupo e a senha para LDAP:

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Criar uma função personalizada com acesso ao endpoint da API REST do usuário S3: `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>` Neste exemplo, a `s3-role` função é gerada para usuários na VM de armazenamento `svm-1` , à qual todos os direitos de acesso, leitura, criação e atualização são concedidos.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

   Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-rest-role-create.html[`security login rest-role create` em referência de comando ONTAP.

3. Crie um grupo de usuários LDAP com o comando de login de segurança e adicione a nova função personalizada para acessar o endpoint da API REST do usuário S3. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-create.html[`security login create`em referência de comando ONTAP.

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

Neste exemplo, o grupo LDAP `ldap-group-1` é criado no `svm-1`, e a função personalizada `s3role` é adicionada a ele para acessar o endpoint da API, juntamente com a habilitação do acesso LDAP no modo de vinculação rápida.

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Para obter mais informações, "Use LDAP fast bind para autenticação nsswitch"consulte .

A adição da função personalizada ao domínio ou grupo LDAP permite aos usuários desse grupo um acesso limitado ao endpoint do ONTAP `/api/protocols/s3/services/{svm.uuid}/users`. Ao invocar a API, os usuários do domínio ou grupo LDAP podem gerar seu próprio acesso e chaves secretas para acessar o cliente S3. Eles podem gerar as chaves apenas para si mesmos e não para outros usuários.

Como um usuário S3 ou LDAP, gere suas próprias chaves de acesso

A partir do ONTAP 9.14,1, você pode gerar seu próprio acesso e chaves secretas para acessar clientes S3, se o administrador lhe concedeu a função de gerar suas próprias chaves. Você pode gerar chaves somente para si mesmo usando o seguinte endpoint da API REST do ONTAP.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir. Para obter informações sobre os outros métodos deste endpoint, consulte a "Documentação do API" referência .

Método HTTP	Caminho
POST	/api/protocols/s3/services/(svm.uuid)/users

Curl exemplo

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Exemplo de saída JSON

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

Ative o acesso do cliente ao armazenamento de objetos S3

Habilite o acesso ao ONTAP S3 para disposição remota de FabricPool em camadas

Para que o ONTAP S3 seja usado como um nível de capacidade remota de FabricPool (nuvem), o administrador do ONTAP S3 deve fornecer informações sobre a configuração do servidor S3 para o administrador remoto do cluster do ONTAP.

Sobre esta tarefa

As seguintes informações do servidor S3 são necessárias para configurar as camadas de nuvem do

FabricPool:

- Nome do servidor (FQDN)
- nome do intervalo
- Certificado CA
- chave de acesso
- palavra-passe (chave de acesso secreta)

Além disso, é necessária a seguinte configuração de rede:

- Deve haver uma entrada para o nome do host do servidor ONTAP S3 remoto no servidor DNS configurado para o SVM admin, incluindo o nome FQDN do servidor S3 e os endereços IP em seus LIFs.
- As LIFs de clusters devem ser configuradas no cluster local, embora o peering de cluster não seja necessário.

Consulte a documentação do FabricPool sobre como configurar o ONTAP S3 como uma camada de nuvem.

"Gerenciamento de camadas de storage usando o FabricPool"

Habilite o acesso ao ONTAP S3 para disposição em camadas local do FabricPool

Para que o ONTAP S3 seja usado como uma categoria de capacidade FabricPool local, você precisa definir um armazenamento de objetos com base no bucket criado e anexá-lo a um agregado de categoria de performance para criar um FabricPool.

Antes de começar

Você deve ter o nome do servidor ONTAP S3 e um nome de bucket, e o servidor S3 deve ter sido criado usando LIFs de cluster (com o `-vserver Cluster` parâmetro).

Sobre esta tarefa

A configuração de armazenamento de objetos contém informações sobre o nível de capacidade local, incluindo os nomes de servidor e bucket do S3 e requisitos de autenticação.

Uma configuração de armazenamento de objetos depois de criada não deve ser reatribuída a um repositório de objetos ou bucket diferente. Você pode criar vários buckets para camadas locais, mas não pode criar vários armazenamentos de objetos em um único bucket.

Não é necessária uma licença FabricPool para um nível de capacidade local.

Passos

1. Crie o armazenamento de objetos para o nível de capacidade local:

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - `-container-name`O é o bucket do S3 que você criou.
   - O `-access-key` parâmetro autoriza solicitações ao servidor ONTAP S3.
   - `-secret-password`O parâmetro (chave de acesso secreto) autentica solicitações ao servidor ONTAP S3.

◦ Você pode definir o `-is-certificate-validation-enabled` parâmetro como `false` para desativar a verificação de certificados para o ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipspace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. Exiba e verifique as informações de configuração do armazenamento de objetos:

   `storage aggregate object-store config show`

3. Opcional: "Determine a quantidade de dados em um volume estão inativos usando relatórios de dados inativos".

   Ver quantos dados em um volume estão inativos pode ajudar você a decidir qual agregado usar para a disposição em camadas local do FabricPool.

4. Anexe o armazenamento de objetos a um agregado:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Você pode usar a `allow-flexgroup` **`true`** opção para anexar agregados que contêm componentes de volume FlexGroup.

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Exiba as informações do armazenamento de objetos e verifique se o armazenamento de objetos anexado está disponível:

   `storage aggregate object-store show`

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

Ative os aplicativos cliente S3 para acessar um servidor ONTAP S3

Para que os aplicativos cliente S3 acessem o servidor ONTAP S3, o administrador do ONTAP S3 deve fornecer informações de configuração ao usuário S3.

Antes de começar

O aplicativo cliente S3 deve ser capaz de autenticar com o servidor ONTAP S3 usando as seguintes versões

de assinatura da AWS:

- Assinatura versão 4, ONTAP 9 .8 e posterior
- Assinatura versão 2, ONTAP 9.11,1 e posterior

Outras versões de assinatura não são suportadas pelo ONTAP S3.

O administrador do ONTAP S3 deve ter criado S3 usuários e concedido permissões de acesso a eles, como usuários individuais ou como membro do grupo, na política de bucket ou na diretiva do servidor de storage de objetos.

O aplicativo cliente S3 deve ser capaz de resolver o nome do servidor ONTAP S3, o que requer que o administrador do ONTAP S3 forneça o nome do servidor S3 (FQDN) e os endereços IP para LIFs do servidor S3.

Sobre esta tarefa

Para acessar um bucket do ONTAP S3, um usuário no aplicativo cliente S3 insere informações fornecidas pelo administrador do ONTAP S3.

A partir do ONTAP 9.9,1, o servidor ONTAP S3 suporta a seguinte funcionalidade de cliente AWS:

- metadados de objetos definidos pelo usuário

  Um conjunto de pares de chave-valor pode ser atribuído a objetos como metadados quando eles são criados usando put (ou POST). Quando uma OPERAÇÃO GET/HEAD é executada no objeto, os metadados definidos pelo usuário são retornados juntamente com os metadados do sistema.

- marcação de objetos

  Um conjunto separado de pares de chave-valor pode ser atribuído como tags para categorizar objetos. Ao contrário dos metadados, as tags são criadas e lidas com APIs REST independentemente do objeto e implementadas quando os objetos são criados ou a qualquer momento depois.

> Para permitir que os clientes obtenham e coloquem informações de marcação, as ações `GetObjectTagging`, `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

Para obter mais informações, consulte a documentação do AWS S3.

Passos

1. Autentique o aplicativo cliente S3 com o servidor ONTAP S3 inserindo o nome do servidor S3 e o certificado da CA.
2. Autentique um usuário no aplicativo cliente S3 inserindo as seguintes informações:
   - Nome do servidor S3 (FQDN) e nome do bucket
   - a chave de acesso e a chave secreta do usuário

Níveis de serviço de storage do ONTAP S3

O ONTAP inclui serviços de storage predefinidos, mapeados para os fatores mínimos de desempenho correspondentes.

O conjunto real de serviços de storage disponíveis em um cluster ou SVM é determinado pelo tipo de storage que compõe o SVM.

A tabela a seguir mostra como os fatores mínimos de desempenho são mapeados para os serviços de storage predefinidos:

Serviço de storage	IOPS esperado (SLA)	IOPS de pico (SLO)	Volume mínimo de IOPS	Latência estimada	As IOPS esperadas são aplicadas?
valor	128 por TB	512 por TB	75	17 ms	No AFF: Sim Caso contrário: Não
desempenho	2048 por TB	4096 por TB	500	2 ms	Sim
extremo	6144 por TB	12288 por TB	1000	1 ms	Sim

A tabela a seguir define o nível de serviço de storage disponível para cada tipo de Mídia ou nó:

Mídia ou nó	Nível de serviço de storage disponível
Disco	valor
Disco da máquina virtual	valor
LUN de FlexArray	valor
Híbrida	valor
Flash otimizado para capacidade	valor
Unidade de estado sólido (SSD) - não-AFF	valor
Flash otimizado para desempenho - SSD (AFF)	extremo, desempenho, valor

Configure o compartilhamento de recursos entre origens (CORS) para buckets do ONTAP S3

A partir do ONTAP 9.16,1, você pode configurar o compartilhamento de recursos entre origens (CORS) para permitir que aplicativos da Web clientes de diferentes domínios acessem seus buckets do ONTAP. Isso fornece acesso seguro aos objetos bucket usando um navegador da Web.

CORS é uma estrutura construída em HTTP que permite que scripts definidos em uma página da Web acessem recursos em um servidor em um domínio diferente. O framework é usado para ignorar com segurança a política *same-origin*, que é uma base inicial para a segurança da web. Os principais conceitos e terminologia são descritos abaixo.

Origem

Uma origem define com precisão a localização e a identidade de um recurso. É representado como uma combinação dos seguintes valores:

- Esquema URI (protocolo)
- Nome de host (nome de domínio ou endereço IP)
- Número da porta

Aqui está um exemplo simples de uma origem: `https://www.mycompany.com:8001`. Quando uma origem é usada com o CORS, ele identifica o cliente que faz a solicitação.

Política da mesma origem

A política de mesma origem (SOP) é um conceito de segurança e restrição aplicados a scripts baseados em navegador. A política permite que scripts carregados inicialmente de uma página da Web acessem dados em outra página, desde que ambas as páginas estejam na mesma origem. Esta limitação impede que scripts maliciosos acessem dados nas páginas de uma origem diferente.

Casos comuns de uso de CORS

Existem vários casos de uso geral para CORS. A maioria envolve instâncias bem definidas de acesso entre domínios, como solicitações AJAX, carregamento de fontes, folhas de estilo e scripts, bem como autenticação entre domínios. O CORS também pode ser implementado como parte de um aplicativo de página única (SPA).

Cabeçalhos HTTP

O CORS é implementado usando cabeçalhos que são inseridos nas solicitações e respostas HTTP. Por exemplo, existem vários cabeçalhos de resposta que implementam o controle de acesso e indicam quais operações, incluindo métodos e cabeçalhos, são permitidas. A presença do cabeçalho *origin* em uma solicitação HTTP o define como uma solicitação de domínio cruzado. O valor de origem é usado pelo servidor CORS para localizar uma configuração CORS válida.

Solicitação HTTP preflight

Esta é uma solicitação opcional para determinar inicialmente se um servidor suporta CORS, incluindo os métodos e cabeçalhos específicos. Com base na resposta, a solicitação do CORS pode ser concluída ou não.

Buckets do ONTAP

Um bucket é um contentor de objetos armazenados e acessados com base em um namespace bem definido. Existem dois tipos de buckets do ONTAP:

- Buckets do nas acessíveis pelos protocolos nas e S3
- Buckets do S3 que só são acessíveis através do protocolo S3

Implementação do CORS em ONTAP

O CORS é ativado por padrão com o ONTAP 9.16,1 e versões posteriores. Você precisa configurar o CORS em cada SVM onde ele estará ativo.

> Não há opção administrativa para desativar o CORS para um cluster ONTAP. No entanto, você pode efetivamente desativá-lo não definindo nenhuma regra ou excluindo todas as regras existentes.

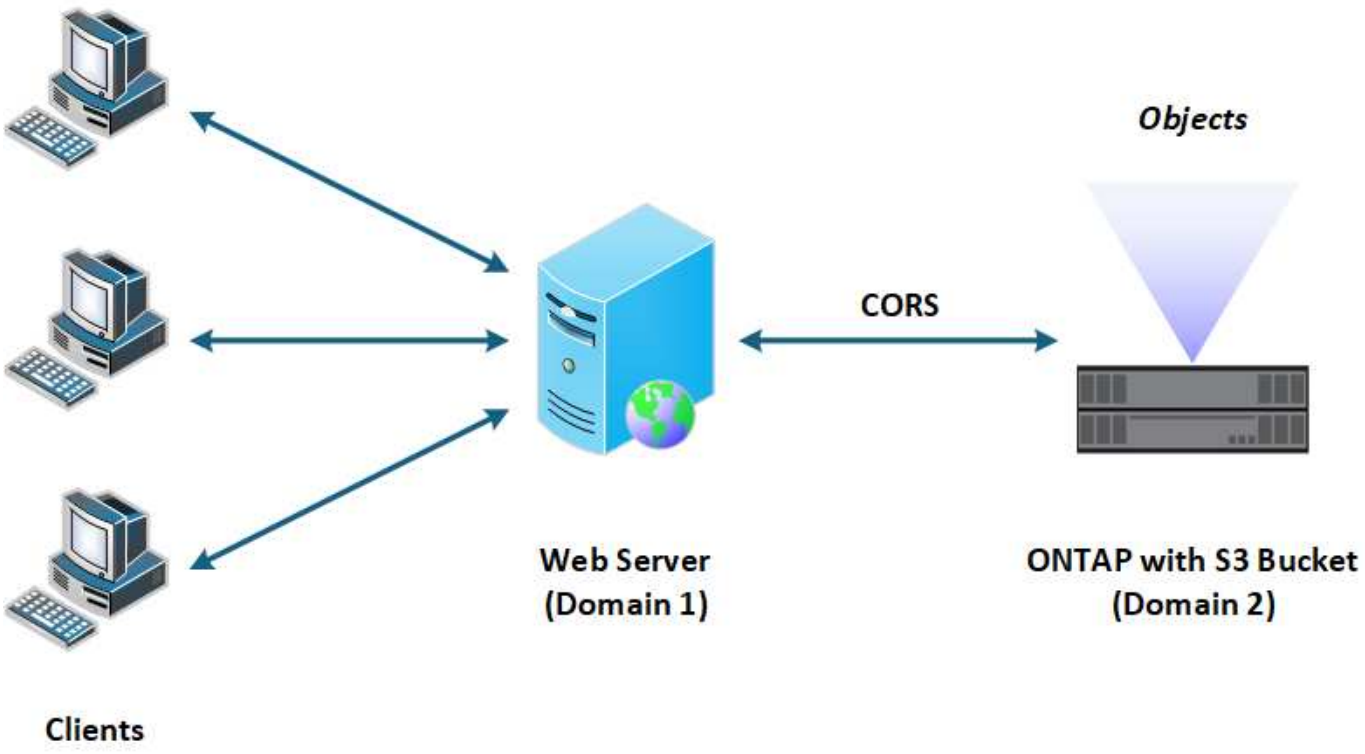
Possíveis casos de uso

A implementação do ONTAP CORS permite várias topologias possíveis para acesso a recursos entre domínios, incluindo:

- Buckets do ONTAP S3 (no mesmo ou diferente SVM ou cluster)
- Buckets do ONTAP nas (no mesmo ou diferente SVM ou cluster)
- Buckets do ONTAP S3 e nas (no mesmo ou diferente SVM ou cluster)
- Buckets do ONTAP e buckets externos de fornecedor
- Baldes em diferentes fusos horários

Vista de alto nível

O seguinte ilustra em alto nível como o CORS permite o acesso aos buckets do ONTAP S3.



Definindo regras CORS

Você precisa definir regras CORS no ONTAP para ativar e usar o recurso.

Ações de configuração

Há três ações principais de regra de configuração suportadas no ONTAP:

- Mostrar
- Criar
- Eliminar

Uma regra CORS definida no ONTAP tem várias propriedades, incluindo o SVM e bucket, bem como as origens, métodos e cabeçalhos permitidos.

Opções de administração

Você tem várias opções disponíveis ao administrar o CORS no cluster do ONTAP.

Interface de linha de comando ONTAP

Você pode configurar o CORS usando a interface de linha de comando. Consulte Administrando CORS usando a CLI para obter mais informações.

API REST do ONTAP

Você pode configurar o CORS usando a API REST do ONTAP. Não foram adicionados novos endpoints para suportar o recurso CORS. Em vez disso, você pode usar o seguinte endpoint existente:

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

Saiba mais no "Documentação de automação do ONTAP".

S3 API

Você pode usar a API S3 para criar e excluir uma configuração CORS em um bucket do ONTAP. Um administrador de cliente S3 requer Privileges suficiente, incluindo:

- Acesso ou credenciais de chave secreta
- Política configurada no bucket para permitir acesso através do s3api

Atualizando e revertendo

Se você planeja usar o CORS para acessar os buckets do ONTAP S3, você deve estar ciente de vários problemas administrativos.

A atualizar

O recurso CORS é suportado quando todos os nós são atualizados para 9.16.1. Em clusters de modo misto, o recurso só estará disponível quando a versão de cluster efetiva (ECV) for 9.16.1 ou posterior.

Reverter

Do ponto de vista do usuário, toda a configuração do CORS deve ser removida antes que a reversão do cluster possa prosseguir. Internamente, a operação excluirá todas as bases de dados CORS. Você será solicitado a executar um comando para limpar e reverter essas estruturas de dados.

Administrando CORS usando a CLI

Você pode usar a CLI do ONTAP para administrar regras do CORS. As operações principais são descritas abaixo. Você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos CORS.

Criar

Você pode definir uma regra CORS usando o `vserver object-store-server bucket cors-rule create` comando.

Parâmetros

Os parâmetros usados para criar uma regra são descritos abaixo.

Parâmetro	Descrição
`vserver`	Especifica o nome do SVM (vserver) que hospeda o bucket do servidor de armazenamento de objetos onde a regra é criada.
`bucket`	O nome do bucket no servidor de armazenamento de objetos para o qual a regra é criada.
`index`	Um parâmetro opcional que indica o índice do bucket do servidor de armazenamento de objetos onde a regra é criada.
`rule id`	Um identificador exclusivo para a regra de bucket do servidor de armazenamento de objetos.
`allowed-origins`	Uma lista das origens das quais os pedidos de origem cruzada são autorizados a ter origem.
`allowed-methods`	Uma lista dos métodos HTTP permitidos em uma solicitação de origem cruzada.
`allowed-headers`	Uma lista dos métodos HTTP permitidos nas solicitações de origem cruzada.
`expose-headers`	Uma lista dos cabeçalhos extras envia nas respostas do CORS que os clientes podem acessar de seus aplicativos.
`max-age-in-seconds`	Um parâmetro opcional especificando a quantidade de tempo que seu navegador deve armazenar em cache uma resposta de pré-voo para um recurso específico.

Exemplo

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

Mostrar

Você pode usar o comando `vserver object-store-server bucket cors-rule show` para exibir uma lista das regras atuais e seu conteúdo.

Incluir o parâmetro `-instance` expande os dados apresentados para cada uma das regras. Você também pode especificar quais campos deseja.

Exemplo

```
server object-store-server bucket cors-rule show -instance
```

Eliminar

Você pode usar o comando delete para remover uma instância de uma regra CORS. Você precisa do `index` valor da regra e, portanto, esta operação é executada em duas etapas:

1. Emita um `show` comando para exibir a regra e recuperar seu índice.
2. Emita a exclusão usando o valor do índice.

Exemplo

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

Modificar

Não há nenhum comando CLI disponível para modificar uma regra CORS existente. Para modificar uma regra, você precisa fazer o seguinte:

1. Exclua a regra existente.
2. Crie uma nova regra com as opções desejadas.

Proteja buckets com o SnapMirror S3

Visão geral do SnapMirror S3

A partir do ONTAP 9.10,1, você pode proteger buckets em armazenamentos de objetos do ONTAP S3 usando a funcionalidade de espelhamento e backup do SnapMirror. Ao contrário do SnapMirror padrão, o SnapMirror S3 permite o espelhamento e os backups para destinos que não sejam NetApp, como o AWS S3.

O SnapMirror S3 é compatível com espelhos ativos e categorias de backup dos buckets do ONTAP S3 nos seguintes destinos:

Alvo	É compatível com espelhos ativos e takeover?	É compatível com backup e restauração?
ONTAP S3 • Buckets no mesmo SVM • Buckets em diferentes SVMs no mesmo cluster • Buckets em SVMs em diferentes clusters	Sim	Sim
StorageGRID	Não	Sim
AWS S3	Não	Sim
Cloud Volumes ONTAP para Azure	Sim	Sim
Cloud Volumes ONTAP para AWS	Sim	Sim
Cloud Volumes ONTAP para Google Cloud	Sim	Sim

Você pode proteger buckets existentes nos servidores do ONTAP S3 ou criar novos buckets com a proteção de dados ativada imediatamente.

Requisitos do SnapMirror S3

- Versão de ONTAP

  O ONTAP 9.10,1 ou posterior deve estar em execução nos clusters de origem e destino.

- Licenciamento

  As seguintes licenças estão disponíveis no "ONTAP One"pacote de software são necessárias em sistemas de origem e destino ONTAP para fornecer acesso a:

  - Protocolo e storage ONTAP S3
  - SnapMirror S3 para segmentar outros destinos de armazenamento de objetos NetApp (ONTAP S3, StorageGRID e Cloud Volumes ONTAP)
  - SnapMirror S3 para segmentar armazenamentos de objetos de terceiros, incluindo AWS S3 (disponível no "Pacote de compatibilidade ONTAP One")

- ONTAP S3
  - Os servidores ONTAP S3 devem estar executando SVMs de origem e destino.
  - Recomenda-se, mas não é necessário, que os certificados de CA para acesso TLS sejam instalados em sistemas que hospedem servidores S3.
    - Os certificados de CA usados para assinar os certificados dos servidores S3 devem ser instalados na VM de armazenamento de administrador dos clusters que hospedam os servidores S3.
    - Você pode usar um certificado de CA autoassinado ou um certificado assinado por um fornecedor de CA externo.
    - Se as VMs de armazenamento de origem ou destino não estiverem escutando em HTTPS, não será necessário instalar certificados de CA.
- Peering (para alvos ONTAP S3)

    - Os LIFs entre clusters devem ser configurados (para destinos ONTAP remotos) e os LIFs entre clusters do cluster de origem e destino podem se conetar às LIFs de dados do servidor S3 de origem e destino.
    - Os clusters de origem e destino são direcionados (para destinos ONTAP remotos).
    - As VMs de armazenamento de origem e destino são direcionadas (para todos os destinos do ONTAP).
- Política de SnapMirror
    - Uma política SnapMirror específica para S3 é necessária para todos os relacionamentos do SnapMirror S3, mas você pode usar a mesma política para vários relacionamentos.
    - Você pode criar sua própria política ou aceitar a política padrão **contínua**, que inclui os seguintes valores:
        - Acelerador (limite superior em taxa de transferência/largura de banda) - ilimitado.
        - Tempo para objetivo do ponto de recuperação: 1 hora (3600 segundos).

> Você deve estar ciente de que quando dois buckets do S3 estiverem em um relacionamento do SnapMirror, se houver políticas de ciclo de vida configuradas para que a versão atual de um objeto expire (seja excluída), a mesma ação será replicada para o bucket do parceiro. Isso é verdade mesmo que o intervalo do parceiro seja somente leitura ou passivo.

- Chaves de usuário raiz armazenamento VM chaves de acesso de usuário raiz são necessárias para relacionamentos do SnapMirror S3; o ONTAP não as atribui por padrão. Na primeira vez que você criar uma relação do SnapMirror S3, você deve verificar se as chaves existem nas VMs de armazenamento de origem e destino e regenerá-las se não o fizerem. Se você precisar regenerá-los, você deve garantir que todos os clientes e todas as configurações de armazenamento de objetos do SnapMirror usando o par de chaves secretas e de acesso sejam atualizados com as novas chaves.

Para obter informações sobre a configuração do servidor S3, consulte os seguintes tópicos:

- "Ative um servidor S3 em uma VM de armazenamento"
- "Sobre o processo de configuração do ONTAP S3"

Para obter informações sobre peering de VM de cluster e armazenamento, consulte o seguinte tópico:

- "Prepare-se para espelhamento e cofre (System Manager, passos 1-6)"
- "Peering de cluster e SVM (CLI)"

Relacionamentos SnapMirror compatíveis

O SnapMirror S3 é compatível com relações em fan-out e cascata. Para obter uma visão geral,"Implantações de proteção de dados em cascata e fan-out"consulte .

O SnapMirror S3 não é compatível com implantações fan-in (relacionamentos de proteção de dados entre vários buckets de origem e um único bucket de destino). O SnapMirror S3 é compatível com vários espelhos de bucket de vários clusters para um único cluster secundário, mas cada bucket do origem deve ter seu próprio bucket do destino no cluster secundário.

Controle o acesso aos buckets do S3

Ao criar novos buckets, você pode controlar o acesso criando usuários e grupos. Para obter mais informações, consulte os seguintes tópicos:

- "Adicionar S3 usuários e grupos (System Manager)"
- "Criar um usuário S3 (CLI)"
- "Criar ou modificar S3 grupos (CLI)"

Proteção de espelho e backup em um cluster remoto

Criar uma relação de espelhamento para um novo bucket (cluster remoto)

Ao criar novos buckets do S3, você pode protegê-los imediatamente em um destino do SnapMirror S3 em um cluster remoto.

Sobre esta tarefa

Você precisará executar tarefas em sistemas de origem e destino.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre clusters de origem e destino, e existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma.
2. Edite a VM de storage para adicionar usuários e adicionar usuários a grupos, nas VMs de armazenamento de origem e destino:

   Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. No cluster de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações**- Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Use os padrões (*bucketname, bucketname/**) ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.

d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**. Em seguida, introduza os seguintes valores:

- Destino
  - **ALVO: Sistema ONTAP**
  - **CLUSTER**: Selecione o cluster remoto.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster remoto.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3:** Copie e cole o conteúdo do certificado *destination*.

5. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
6. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
7. Clique em **Salvar**. Um novo bucket é criado na VM de storage de origem e é espelhado em um novo bucket que é criado a VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:

   ```
   vserver object-store-server user show
   ```

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   Não regenere a chave se já existir uma.

2. Crie buckets nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   ```

`[additional_options]`

3. Adicione regras de acesso às políticas de bucket padrão nas SVMs de origem e de destino:

   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. No SVM de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros:

   - Tipo `continuous` - o único tipo de política para relacionamentos SnapMirror S3 (obrigatório).
   - `-rpo` - especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` - especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

     Exemplo

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instalar certificados de servidor CA nas SVMs administrativas dos clusters de origem e destino:

   a. No cluster de origem, instale o certificado da CA que assinou o certificado do servidor *Destination* S3:
      `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. No cluster de destino, instale o certificado da CA que assinou o certificado do servidor *source* S3:
      `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

      Se você estiver usando um certificado assinado por um fornecedor de CA externo, instale o mesmo certificado na SVM do administrador de origem e destino.

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Na fonte SVM, crie uma relação do SnapMirror S3:

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   Você pode usar uma política criada ou aceitar o padrão.

   Exemplo

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
   test-policy
   ```

7. Verifique se o espelhamento está ativo:
   `snapmirror show -policy-type continuous -fields status`

Criar uma relação de espelhamento para um bucket existente (cluster remoto)

Você pode começar a proteger os buckets existentes do S3 a qualquer momento; por exemplo, se você atualizou uma configuração do S3 de uma versão anterior ao ONTAP 9.10,1.

Sobre esta tarefa

Você precisa executar tarefas nos clusters de origem e destino.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre clusters de origem e destino, e existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

Passos

Você pode criar uma relação de espelhamento usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Selecione **Storage > Storage VMs** e, em seguida, selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key.** Não regenere a chave se já existir uma.
2. Verifique se os usuários e grupos existentes estão presentes e têm o acesso correto nas VMs de armazenamento de origem e destino: Selecione **armazenamento > VMs de armazenamento** e, em seguida, selecione a VM de armazenamento e, em seguida, a guia **Configurações**. Por fim, localize o bloco **S3**, selecione e selecione a guia **usuários** e, em seguida, a guia **grupos** para exibir as configurações de acesso de usuário e grupo.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. No cluster de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Selecione **proteção > Visão geral** e clique em **Configurações de política local**.
   b. Selecione ao lado de **políticas de proteção** e clique em **Adicionar**.
   c. Introduza o nome e a descrição da política.
   d. Selecione o escopo da política, cluster ou SVM.
   e. Selecione **contínuo** para relações SnapMirror S3.
   f. Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Verifique se a política de acesso ao bucket do bucket existente ainda atende às suas necessidades:
   a. Clique em **armazenamento > baldes** e, em seguida, selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal e efeito**: Selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações**: Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos**: Use os padrões (*bucketname, bucketname/**) ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Proteja um balde existente com proteção SnapMirror S3:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.
   b. Clique em **Protect** e insira os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster remoto.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster remoto.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *destination*.

6. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
7. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
8. Clique em **Salvar**. O bucket existente é espelhado em um novo bucket na VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se esta for a primeira relação do SnapMirror S3 para este SVM, verifique se existem chaves de usuário raiz para SVMs de origem e de destino e regenere-as se não o fizerem:
   `vserver object-store-server user show` Se não houver, digite:
   `vserver object-store-server user regenerate-keys -vserver` *`svm_name`* `-user` *`root`* Não regenere a chave se já existir.
2. Crie um bucket no SVM de destino para ser o destino espelhado:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Verifique se as regras de acesso das políticas de bucket padrão estão corretas nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

Exemplo

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. No SVM de origem, crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros:

   - `continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório).
   - `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

     Exemplo

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instalar certificados de CA nas SVMs administrativas dos clusters de origem e destino:

   a. No cluster de origem, instale o certificado da CA que assinou o certificado do servidor *Destination* S3:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. No cluster de destino, instale o certificado da CA que assinou o certificado do servidor *source* S3:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` Se você estiver usando um certificado assinado por um fornecedor de CA externo, instale o mesmo certificado no SVM do administrador de origem e destino.

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Na fonte SVM, crie uma relação do SnapMirror S3:

   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Você pode usar uma política criada ou aceitar o padrão.

Exemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Takeover e fornecimento de dados do bucket do destino (cluster remoto)

Se os dados em um bucket de origem ficarem indisponíveis, você poderá interromper a relação do SnapMirror para tornar o bucket de destino gravável e começar a fornecer dados.

Sobre esta tarefa

Quando uma operação de aquisição é executada, o bucket de origem é convertido em somente leitura e o bucket de destino original é convertido em leitura-gravação, revertendo assim a relação do SnapMirror S3.

Quando o bucket de origem desativado estiver disponível novamente, o SnapMirror S3 ressincroniza automaticamente o conteúdo dos dois buckets. Não é necessário ressincronizar explicitamente a relação, como é necessário para implantações de volume SnapMirror.

A operação de aquisição deve ser iniciada a partir do cluster remoto.

System Manager

Faça failover do bucket indisponível e comece a fornecer dados:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em , selecione **failover** e, em seguida, clique em **failover**.

CLI

1. Inicie uma operação de failover para o bucket de destino:
`snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verifique o status da operação de failover:
`snapmirror show -fields status`

Exemplo

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

Restaurar um bucket da VM de armazenamento de destino (cluster remoto)

Se os dados em um bucket de origem forem perdidos ou corrompidos, você poderá

preencher novamente os dados restaurando objetos de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O intervalo de destino para a operação de restauração deve ser maior do que o espaço lógico usado do intervalo de destino.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

A operação de restauração deve ser iniciada a partir do cluster remoto.

System Manager

Restaure os dados de cópia de segurança:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
     - Copie e cole o conteúdo do certificado da CA do servidor *destination* S3.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA do servidor *destination* S3.
4. Em **destino**, copie e cole o conteúdo do certificado da CA do servidor *source* S3.
5. Clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

Restaure os baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets bloqueados e restaurá-los conforme necessário.

Você pode restaurar um bucket bloqueado por objeto para um bucket novo ou existente. Você pode selecionar um bucket bloqueado por objeto como destino nos seguintes cenários:

- **Restaurar para um novo bucket**: Quando o bloqueio de objetos está ativado, um bucket pode ser restaurado criando um bucket que também tem o bloqueio de objetos ativado. Ao restaurar um bucket bloqueado, o modo de bloqueio de objetos e o período de retenção do bucket original são replicados. Também pode definir um período de retenção de bloqueio diferente para o novo balde. Este período de retenção é aplicado a objetos não bloqueados de outras fontes.
- **Restaurar para um bucket existente**: Um bucket bloqueado por objeto pode ser restaurado para um bucket existente, desde que o controle de versão e um modo de bloqueio de objeto semelhante estejam ativados no bucket existente. O período de retenção do balde original é mantido.
- **Restaurar bucket não bloqueado**: Mesmo que o bloqueio de objetos não esteja habilitado em um bucket, você pode restaurá-lo para um bucket que tenha o bloqueio de objetos ativado e esteja no cluster de origem. Quando você restaura o bucket, todos os objetos não bloqueados ficam bloqueados e o modo de retenção e a posse do bucket de destino se aplicam a eles.

CLI

1. Crie o novo intervalo de destino para restauração. Para obter mais informações, "Criar um relacionamento de backup para um novo bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*

Exemplo

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

Proteção de espelho e backup no cluster local

Criar uma relação de espelho para um novo bucket (cluster local)

Ao criar novos buckets do S3, você pode protegê-los imediatamente para um destino do SnapMirror S3 no mesmo cluster. É possível espelhar dados em um bucket em uma VM de storage diferente ou na mesma VM de storage que a origem.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Configurações**, clique no bloco S3.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma.
2. Edite a VM de armazenamento para adicionar usuários e adicionar usuários a grupos, tanto nas VMs de armazenamento de origem quanto de destino: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e depois em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Use os padrões `(bucketname, bucketname/*)` ou outros valores que você precisa

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
   d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**. Em seguida, introduza os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster local.
  - **STORAGE VM**: Selecione uma VM de armazenamento no cluster local.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado de origem.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado de destino.

5. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
6. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
7. Clique em **Salvar**. Um novo bucket é criado na VM de storage de origem e é espelhado em um novo bucket que é criado a VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:
   `vserver object-store-server user show`

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Não regenere a chave se já existir uma.

2. Crie buckets nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Adicione regras de acesso às políticas de bucket padrão nas SVMs de origem e de destino:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   ```

`-principal` *`user_and_group_names`* `-resource` *`object_store_resources`* `[-sid` *`text`*`] [-index` *`integer`*`]`

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   Parâmetros:

   - `continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório).
   - `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Instalar certificados de servidor da CA no SVM do administrador:
   a. Instale o certificado da CA que assinou o certificado do servidor *source* S3 no SVM do administrador:
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`src_server_certificate`*
   b. Instale o certificado da CA que assinou o certificado do servidor *destino* S3 no SVM admin:
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`dest_server_certificate`* Se você estiver usando um certificado assinado por um fornecedor externo de CA, você só precisará instalar esse certificado no SVM do administrador.

      Consulte a `security certificate install` página de manual para obter detalhes.

6. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]``

   Você pode usar uma política criada ou aceitar o padrão.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

7. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Criar uma relação de espelhamento para um bucket existente (cluster local)

Você pode começar a proteger buckets S3 existentes no mesmo cluster a qualquer momento; por exemplo, se você atualizou uma configuração S3 de uma versão anterior ao ONTAP 9.10,1. É possível espelhar dados em um bucket em uma VM de storage diferente ou na mesma VM de storage que a origem.

Antes de começar

- Os requisitos para versões do ONTAP, licenciamento e configuração do servidor S3 foram concluídos.
- Existe uma relação de peering entre VMs de armazenamento de origem e destino.
- Os certificados de CA são necessários para as VMs de origem e destino. Você pode usar certificados de CA autoassinados ou certificados assinados por um fornecedor de CA externo.

System Manager

1. Se essa for a primeira relação do SnapMirror S3 para essa VM de storage, verifique se existem chaves de usuário raiz para as VMs de armazenamento de origem e destino e regenere-as se não:
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Na guia **Settings**, clique no mosaico **S3**.
   c. Na guia **usuários**, verifique se há uma chave de acesso para o usuário raiz.
   d. Se não existir, clique em junto a **root** e, em seguida, clique em **Regenerate Key**. Não regenere a chave se já existir uma
2. Verifique se os usuários e grupos existentes estão presentes e têm o acesso correto nas VMs de armazenamento de origem e destino: Selecione **armazenamento > VMs de armazenamento** e, em seguida, selecione a VM de armazenamento e, em seguida, a guia **Configurações**. Por fim, localize o bloco **S3**, selecione e selecione a guia **usuários** e, em seguida, a guia **grupos** para exibir as configurações de acesso de usuário e grupo.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configuração de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Verifique se a política de acesso ao bucket do bucket existente continua atendendo às suas necessidades:
   a. Clique em **armazenamento > baldes** e, em seguida, selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Use os padrões *(bucketname, bucketname/*)* ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Proteja um balde existente com o SnapMirror S3:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.

b. Clique em **Protect** e insira os seguintes valores:

- Destino
  - **ALVO**: Sistema ONTAP
  - **CLUSTER**: Selecione o cluster local.
  - **STORAGE VM**: Selecione a mesma ou outra VM de armazenamento.
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *source*.
- Fonte
  - **CERTIFICADO CA DE SERVIDOR S3**: Copie e cole o conteúdo do certificado *destination*.

6. Marque **Use o mesmo certificado no destino** se estiver usando um certificado assinado por um fornecedor externo de CA.
7. Se clicar em **Destination Settings** (Definições de destino), também poderá introduzir os seus próprios valores em vez dos padrões para o nome do intervalo, capacidade e nível de serviço de desempenho.
8. Clique em **Salvar**. O bucket existente é espelhado em um novo bucket na VM de storage de destino.

Faça backup de baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets S3 bloqueados e restaurá-los conforme necessário.

Ao definir as configurações de proteção para um bucket novo ou existente, é possível ativar o bloqueio de objetos nos buckets de destino, desde que os clusters de origem e destino executem o ONTAP 9.14,1 ou posterior e que o bloqueio de objetos esteja ativado no bucket de origem. O modo de bloqueio de objetos e a posse de retenção de bloqueio do bucket de origem se tornam aplicáveis aos objetos replicados no bucket de destino. Você também pode definir um período de retenção de bloqueio diferente para o intervalo de destino na seção **Configurações de destino**. Esse período de retenção também é aplicado a quaisquer objetos não bloqueados replicados a partir do bucket de origem e das interfaces S3.

Para obter informações sobre como ativar o bloqueio de objetos em um balde, "Crie um bucket"consulte .

CLI

1. Se essa for a primeira relação do SnapMirror S3 para esse SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e as regenere se não:
   `vserver object-store-server user show`

   Verifique se há uma chave de acesso para o usuário raiz. Se não existir, introduza:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Não regenere a chave se já existir uma.

2. Crie um bucket no SVM de destino para ser o destino espelhado:

   `vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. Verifique se as regras de acesso às políticas de bucket padrão estão corretas nas SVMs de origem e de destino:

`vserver object-store-server bucket policy add-statement -vserver *svm_name* -bucket *bucket_name* -effect {allow|deny} -action *object_store_actions* -principal *user_and_group_names* -resource *object_store_resources* [-sid *text*] [-index *integer*]`

Exemplo

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:

   `snapmirror policy create -vserver *svm_name* -policy *policy_name* -type *continuous [-rpo _integer*] [-throttle *throttle_type*] [-comment text] [*additional_options*]`

   Parâmetros:

   - `continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório).
   - `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional).
   - `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

     Exemplo

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instalar certificados de servidor da CA no SVM do administrador:
   a. Instale o certificado da CA que assinou o certificado do servidor *source* S3 no SVM do administrador:
      `security certificate install -type server-ca -vserver *admin_svm* -cert -name *src_server_certificate*`
   b. Instale o certificado da CA que assinou o certificado do servidor *destino* S3 no SVM admin:
      `security certificate install -type server-ca -vserver *admin_svm* -cert -name *dest_server_certificate*` Se você estiver usando um certificado assinado por um fornecedor externo de CA, você só precisará instalar esse certificado no SVM do administrador.

      Consulte a `security certificate install` página de manual para obter detalhes.

6. Criar uma relação do SnapMirror S3:
   `snapmirror create -source-path *src_svm_name*:/bucket/*bucket_name* -destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

Você pode usar uma política criada ou aceitar o padrão.

Exemplo

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Takeover e fornecimento de dados do bucket do destino (cluster local)

Se os dados em um bucket de origem ficarem indisponíveis, você poderá interromper a relação do SnapMirror para tornar o bucket de destino gravável e começar a fornecer dados.

Sobre esta tarefa

Quando uma operação de aquisição é executada, o bucket de origem é convertido em somente leitura e o bucket de destino original é convertido em leitura-gravação, revertendo assim a relação do SnapMirror S3.

Quando o bucket de origem desativado estiver disponível novamente, o SnapMirror S3 ressincroniza automaticamente o conteúdo dos dois buckets. Não é necessário ressincronizar explicitamente a relação, como é necessário para implantações padrão de volume SnapMirror.

Se o intervalo de destino estiver em um cluster remoto, a operação de aquisição deve ser iniciada a partir do cluster remoto.

System Manager

Faça failover do bucket indisponível e comece a fornecer dados:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em , selecione **failover** e, em seguida, clique em **failover**.

CLI

1. Inicie uma operação de failover para o bucket de destino:
`snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verifique o status da operação de failover:
`snapmirror show -fields status`

Exemplo

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Restaurar um bucket da VM de armazenamento de destino (cluster local)

Quando os dados em um bucket de origem são perdidos ou corrompidos, você pode

preencher novamente seus dados restaurando objetos de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O intervalo de destino para a operação de restauração deve ser maior que o intervalo de destino;s espaço lógico usado.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

A operação de restauração deve ser iniciada a partir do cluster local.

System Manager

Restaure os dados de backup:

1. Clique em **proteção > relacionamentos** e, em seguida, selecione o intervalo.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
4. Copie e cole o conteúdo do certificado de CA do servidor S3 de destino.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA de servidor S3 de destino.
5. Em **destino**, copie e cole o conteúdo do certificado de CA do servidor S3 de origem.
6. Clique em **proteção** > relacionamentos para monitorar o progresso da restauração.

Restaure os baldes bloqueados

A partir do ONTAP 9.14,1, você pode fazer backup de buckets bloqueados e restaurá-los conforme necessário.

Você pode restaurar um bucket bloqueado por objeto para um bucket novo ou existente. Você pode selecionar um bucket bloqueado por objeto como destino nos seguintes cenários:

- **Restaurar para um novo bucket**: Quando o bloqueio de objetos está ativado, um bucket pode ser restaurado criando um bucket que também tem o bloqueio de objetos ativado. Ao restaurar um bucket bloqueado, o modo de bloqueio de objetos e o período de retenção do bucket original são replicados. Também pode definir um período de retenção de bloqueio diferente para o novo balde. Este período de retenção é aplicado a objetos não bloqueados de outras fontes.
- **Restaurar para um bucket existente**: Um bucket bloqueado por objeto pode ser restaurado para um bucket existente, desde que o controle de versão e um modo de bloqueio de objeto semelhante estejam ativados no bucket existente. O período de retenção do balde original é mantido.
- **Restaurar bucket não bloqueado**: Mesmo que o bloqueio de objetos não esteja habilitado em um bucket, você pode restaurá-lo para um bucket que tenha o bloqueio de objetos ativado e esteja no cluster de origem. Quando você restaura o bucket, todos os objetos não bloqueados ficam bloqueados e o modo de retenção e a posse do bucket de destino se aplicam a eles.

CLI

1. Se você estiver restaurando objetos para um novo bucket, crie o novo bucket. Para obter mais informações, "Criar um relacionamento de backup para um novo bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

Exemplo

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

Proteção de backup com destinos em nuvem

Requisitos para relacionamentos de destino na nuvem

Certifique-se de que seus ambientes de origem e destino atendam aos requisitos de proteção de backup do SnapMirror S3 para destinos na nuvem.

Você deve ter credenciais de conta válidas com o provedor de armazenamento de objetos para acessar o intervalo de dados.

LIFs entre clusters e um espaço IPspace devem ser configurados no cluster antes que o cluster possa se conetar a um armazenamento de objetos em nuvem. Você deve criar LIFs entre clusters em cada nó para transferir dados de forma otimizada do storage local para o armazenamento de objetos em nuvem.

Para alvos StorageGRID, você precisa saber as seguintes informações:

- Nome do servidor, expresso como um nome de domínio totalmente qualificado (FQDN) ou endereço IP
- nome do bucket; o bucket já deve existir
- chave de acesso
- chave secreta

Além disso, o certificado da CA usado para assinar o certificado do servidor StorageGRID precisa ser instalado na VM de armazenamento de administrador do cluster do ONTAP S3 usando o `security certificate install command`. Para obter mais informações, consulte "Instalando um certificado CA" se você usa o StorageGRID.

Para os destinos do AWS S3, você precisa saber as seguintes informações:

- Nome do servidor, expresso como um nome de domínio totalmente qualificado (FQDN) ou endereço IP
- nome do bucket; o bucket já deve existir
- chave de acesso
- chave secreta

O servidor DNS para a VM de armazenamento de administrador do cluster ONTAP deve ser capaz de resolver FQDNs (se usado) para endereços IP.

Criar um relacionamento de backup para um novo bucket (destino na nuvem)

Ao criar novos buckets do S3, você pode fazer backup deles imediatamente em um bucket de destino do SnapMirror S3 em um provedor de armazenamento de objetos, que pode ser um sistema StorageGRID ou uma implantação do Amazon S3.

Antes de começar

- Você tem credenciais de conta válidas e informações de configuração para o provedor de armazenamento de objetos.
- Interfaces de rede entre clusters e um IPspace foram configurados no sistema de origem.
- • A configuração DNS para a VM de armazenamento de origem deve ser capaz de resolver o FQDN do destino.

System Manager

1. Edite a VM de armazenamento para adicionar usuários e para adicionar usuários a grupos:
   a. Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em **S3**.

      Consulte "Adicione S3 usuários e grupos" para obter mais informações.

2. Adicione um Cloud Object Store no sistema de origem:
   a. Clique em **proteção > Visão geral** e selecione **Cloud Object Stores**.
   b. Clique em **Adicionar** e selecione **Amazon S3** ou **StorageGRID**.
   c. Introduza os seguintes valores:
      - Nome do armazenamento de objetos na nuvem
      - Estilo de URL (caminho ou virtual-hospedado)
      - VM de armazenamento (ativada para S3)
      - Nome do servidor de armazenamento de objetos (FQDN)
      - Certificado de armazenamento de objetos
      - Chave de acesso
      - Chave secreta
      - Nome do recipiente (balde)
3. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique → ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
      - Introduza o nome e a descrição da política.
      - Selecione o escopo da política, o cluster ou o SVM
      - Selecione **contínuo** para relações SnapMirror S3.
      - Introduza os valores **Throttle** e **Recovery Point Objective**.
4. Crie um balde com proteção SnapMirror:
   a. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento, insira um tamanho e clique em **mais Opções**.
   c. Em **permissões**, clique em **Adicionar**. Verificar permissões é opcional, mas recomendado.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados:

        ```
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
        bjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
        ```

      - **Recursos** - Use os padrões `_(bucketname, bucketname/*)` ou outros valores que você

precisa.

Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.

d. Em **proteção**, marque **Ativar SnapMirror (ONTAP ou nuvem)**, selecione **armazenamento em nuvem** e, em seguida, selecione **armazenamento de objetos em nuvem**.

Quando você clica em **Salvar**, um novo bucket é criado na VM de armazenamento de origem e é feito o backup no armazenamento de objetos na nuvem.

CLI

1. Se esta for a primeira relação do SnapMirror S3 para este SVM, verifique se as chaves de usuário raiz existem para SVMs de origem e destino e regenere-as se não o fizerem:
`vserver object-store-server user show` Confirme que há uma chave de acesso para o usuário raiz. Se não houver, digite:
`vserver object-store-server user regenerate-keys -vserver svm_name -user root` Não regenere a chave se já existir.
2. Crie um bucket no SVM de origem:
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. Adicione regras de acesso à política de bucket padrão:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros: * `type continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório). * `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional). * `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

Exemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. Se o destino for um sistema StorageGRID, instale o certificado do servidor da CA StorageGRID no SVM admin do cluster de origem:
`security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   Consulte a `security certificate install` página de manual para obter detalhes.

6. Defina o armazenamento de objetos de destino do SnapMirror S3:
`snapmirror object-store config create -vserver` *`svm_name`* `-object-store-name` *`target_store_name`* `-usage data -provider-type {AWS_S3|SGWS} -server` *`target_FQDN`* `-container-name` *`remote_bucket_name`* `-is-ssl-enabled true -port` *`port_number`* `-access-key target_access_key -secret-password` *`target_secret_key`*

   Parâmetros: * `-object-store-name` – O nome do alvo do armazenamento de objetos no sistema ONTAP local. * `-usage` – use `data` para este fluxo de trabalho. * `-provider-type` – `AWS_S3` E `SGWS` (StorageGRID) alvos são suportados. `-server`* – O FQDN ou endereço IP do servidor de destino. * `-is-ssl-enabled` –Ativar SSL é opcional, mas recomendado. Veja a `snapmirror object-store config create` página de manual para mais detalhes.

   Exemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

   Parâmetros: * `-destination-path` - O nome do armazenamento de objetos que você criou na etapa anterior e o valor fixo `objstore` . Você pode usar uma política que você criou ou aceitar o padrão.

   Exemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Criar um relacionamento de backup para um bucket existente (destino na nuvem)

Você pode começar a fazer backup de buckets S3 existentes a qualquer momento; por exemplo, se você atualizou uma configuração S3 de uma versão anterior ao ONTAP 9.10,1.

Antes de começar

- Você tem credenciais de conta válidas e informações de configuração para o provedor de armazenamento de objetos.
- Interfaces de rede entre clusters e um IPspace foram configurados no sistema de origem.
- A configuração DNS para a VM de armazenamento de origem deve ser capaz de resolver o FQDN do destino.

System Manager

1. Verifique se os usuários e grupos estão definidos corretamente: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em abaixo de S3.

   Consulte "Adicione S3 usuários e grupos" para obter mais informações.

2. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
   a. Clique em **proteção > Visão geral** e, em seguida, clique em **Configurações de política local**.
   b. Clique ao lado de **políticas de proteção** e, em seguida, clique em **Adicionar**.
   c. Introduza o nome e a descrição da política.
   d. Selecione o escopo da política, o cluster ou o SVM
   e. Selecione **contínuo** para relações SnapMirror S3.
   f. Insira os valores de objetivo **Throttle** e **ponto de recuperação**.
3. Adicione um Cloud Object Store no sistema de origem:
   a. Clique em **proteção > Visão geral** e selecione **Cloud Object Store**.
   b. Clique em **Adicionar** e selecione **Amazon S3** ou **outros** para o StorageGRID Webscale.
   c. Introduza os seguintes valores:
      - Nome do armazenamento de objetos na nuvem
      - Estilo de URL (caminho ou virtual-hospedado)
      - VM de armazenamento (ativada para S3)
      - Nome do servidor de armazenamento de objetos (FQDN)
      - Certificado de armazenamento de objetos
      - Chave de acesso
      - Chave secreta
      - Nome do recipiente (balde)
4. Verifique se a política de acesso ao bucket do bucket existente ainda atende às suas necessidades:
   a. Clique em **armazenamento** > **baldes** e selecione o balde que pretende proteger.
   b. Na guia **permissões**, clique em **Editar** e, em seguida, clique em **Adicionar** em **permissões**.
      - **Principal** e **efeito** - selecione os valores correspondentes às configurações do grupo de usuários ou aceite os padrões.
      - **Ações** - Certifique-se de que os seguintes valores são mostrados: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Recursos** - Use os padrões *`(bucketname, bucketname/*)`* ou outros valores que você precisa.

        Consulte "Gerenciar o acesso do usuário aos buckets" para obter mais informações sobre esses campos.
5. Faça backup do balde usando o SnapMirror S3:

a. Clique em **Storage** > **Buckets** e selecione o bucket que deseja fazer backup.

b. Clique em **Protect**, selecione **Cloud Storage** em **Target** e, em seguida, selecione **Cloud Object Store**.

Quando você clica em **Salvar**, o bucket existente é feito o backup no armazenamento de objetos na nuvem.

CLI

1. Verifique se as regras de acesso na política de bucket padrão estão corretas:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Exemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. Crie uma política do SnapMirror S3 se você não tiver uma política existente e não quiser usar a política padrão:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parâmetros: * `type continuous` – O único tipo de política para relações SnapMirror S3 (obrigatório). * `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos (opcional). * `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos (opcional).

   Exemplo

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. Se o destino for um sistema StorageGRID, instale o certificado da CA StorageGRID no SVM de administrador do cluster de origem:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Consulte a `security certificate install` página de manual para obter detalhes.

4. Defina o armazenamento de objetos de destino do SnapMirror S3:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password`

target_secret_key

Parâmetros: * `-object-store-name` – O nome do alvo do armazenamento de objetos no sistema ONTAP local. * `-usage` – use `data` para este fluxo de trabalho. * `-provider-type` – `AWS_S3` E `SGWS` (StorageGRID) alvos são suportados. `-server`* – O FQDN ou endereço IP do servidor de destino. * `-is-ssl-enabled` –Ativar SSL é opcional, mas recomendado. Veja a `snapmirror object-store config create` página de manual para mais detalhes.

Exemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Criar uma relação do SnapMirror S3:
`snapmirror create -source-path *svm_name*:/bucket/*bucket_name* -destination -path *object_store_name*:/objstore -policy *policy_name*`

   Parâmetros: * `-destination-path` - O nome do armazenamento de objetos que você criou na etapa anterior e o valor fixo `objstore` . Você pode usar uma política que você criou ou aceitar o padrão.

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
   -destination-path sgws-store:/objstore -policy test-policy
   ```

6. Verifique se o espelhamento está ativo:
`snapmirror show -policy-type continuous -fields status`

Restaurar um bucket do destino na nuvem

Quando os dados em um bucket de origem são perdidos ou corrompidos, você pode preencher novamente seus dados restaurando de um bucket de destino.

Sobre esta tarefa

Você pode restaurar o intervalo de destino para um bucket existente ou um novo bucket. O bucket de destino para a operação de restauração deve ser maior que o espaço lógico usado do bucket de destino.

Se você usar um bucket existente, ele deve estar vazio ao iniciar uma operação de restauração. Restaurar não "reverte" um balde no tempo; em vez disso, ele preenche um balde vazio com seu conteúdo anterior.

System Manager

Restaure os dados de backup:

1. Clique em **proteção > relacionamentos** e selecione **SnapMirror S3**.
2. Clique em e selecione **Restore**.
3. Em **Source**, selecione **existing Bucket** (o padrão) ou **New Bucket**.
   - Para restaurar para um **Bucket existente** (o padrão), execute estas ações:
     - Selecione o cluster e a VM de armazenamento para procurar o bucket existente.
     - Selecione o balde existente.
     - Copie e cole o conteúdo do certificado da CA do servidor *destination* S3.
   - Para restaurar um **novo balde**, insira os seguintes valores:
     - O cluster e a VM de storage para hospedar o novo bucket.
     - Nome, capacidade e nível de serviço de performance do novo bucket. Consulte "Níveis de serviço de storage" para obter mais informações.
     - O conteúdo do certificado de CA de servidor S3 de destino.
4. Em **destino**, copie e cole o conteúdo do certificado da CA do servidor *source* S3.
5. Clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

Procedimento CLI

1. Crie o novo intervalo de destino para restauração. Para obter mais informações, "Criar um relacionamento de backup para um bucket (destino na nuvem)"consulte .
2. Inicie uma operação de restauração para o intervalo de destino:
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   Exemplo

   O exemplo a seguir restaura um bucket de destino para um bucket existente.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

Modificar uma política de espelho

Você pode querer modificar uma política de espelhamento do S3; por exemplo, se quiser ajustar os valores de RPO e acelerador.

System Manager

Se você quiser ajustar esses valores, você pode editar uma política de proteção existente.

1. Clique em **proteção > relacionamentos** e, em seguida, selecione a política de proteção para o relacionamento que deseja modificar.
2. Clique ⋮ ao lado do nome da política e, em seguida, clique em **Editar**.

CLI

Modificar uma política do SnapMirror S3:
`snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer] [-throttle throttle_type] [-comment text]`

Parâmetros:

- `-rpo` – especifica o tempo para o objetivo do ponto de recuperação, em segundos.
- `-throttle` – especifica o limite superior na taxa de transferência/largura de banda, em kilobytes/segundos.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Proteger dados do S3 com snapshots

Visão geral do instantâneo do S3

A partir do ONTAP 9.16,1, você pode usar a tecnologia de snapshot do ONTAP para gerar imagens pontuais e somente leitura dos buckets do ONTAP S3.

Usando o recurso snapshots S3, você pode criar snapshots manualmente ou gerá-los automaticamente por meio de políticas de snapshot. Os snapshots S3 são apresentados como buckets S3 para S3 clientes. Você pode navegar e restaurar o conteúdo dos instantâneos através de clientes S3.

No ONTAP 9.16,1, os snapshots S3 capturam apenas as versões atuais dos objetos em buckets do S3. As versões não atuais dos buckets versionados não são capturadas nos snapshots S3. Além disso, as tags de objeto point-in-time não são capturadas nos snapshots se as tags de objeto forem modificadas após as capturas instantâneas serem tiradas.

S3 snapshots dependem do tempo do cluster. Você deve configurar o servidor NTP no cluster para sincronizar a hora. Para obter mais informações, "Gerenciar o tempo do cluster"consulte .

Uso de cota e espaço

As cotas rastreiam o número de objetos e o tamanho lógico usados em um bucket do S3. Quando são criados instantâneos S3D, os objetos capturados nos instantâneos S3D são contados em direção à contagem e ao tamanho de objetos de bucket usados, até que os instantâneos sejam excluídos do sistema de arquivos.

Objetos multiparte

Para objetos multiparte, apenas os objetos finais são capturados em instantâneos. Uploads parciais de

objetos multipart não são capturados em snapshots.

Snapshots em buckets versionados e não versionados

Você pode criar snapshots em buckets versionados e não versionados. O instantâneo contém apenas as versões atuais do objeto em um momento em que o instantâneo é capturado.

Buckets e snapshots versionados

Em buckets com o controle de versão de objeto habilitado, um snapshot retém o conteúdo da versão de objeto mais recente após a qual o snapshot foi capturado. Exclui versões não atuais no balde.

Considere este exemplo: Em um bucket onde o controle de versão do objeto está habilitado, o objeto `obj1` tem as versões v1, v2, v3, v4, v5. Você criou um instantâneo `snap1` a partir `obj1` de v3 (a versão mais recente no ponto de captura). Ao navegar `snap1`, `obj1` aparecerá como um objeto com conteúdo criado em v3. O conteúdo das versões anteriores não será devolvido.

> As versões não atuais são mantidas no sistema de arquivos, até que os snapshots sejam excluídos.

Buckets e snapshots não versionados

Em buckets não versionados, os snapshots S3 preservam o conteúdo dos commits mais recentes antes da criação do snapshot.

Considere este exemplo: Em um bucket onde o controle de versão de objetos não está disponível, o objeto `obj1` foi substituído várias vezes em (T1, T2, T3, T4 e T5). Você criou um snapshot S3 `snap1` em algum momento entre T3 e T4. Ao navegar `snap1`, `obj1` aparecerá com o conteúdo criado em T3.

Expiração de objetos e snapshots

A expiração de objetos do ONTAP S3 e os snapshots S3 funcionam independentemente um do outro. O recurso de expiração de objeto do ONTAP expira as versões de objeto de acordo com as regras de gerenciamento de ciclo de vida definidas para o bucket do S3. Os snapshots S3 são cópias estáticas dos objetos bucket em um momento em que o snapshot é criado.

Se o controle de versão do objeto estiver habilitado em um bucket, quando uma versão específica de um objeto for excluída devido a uma regra de expiração definida para esse bucket, o conteúdo da versão expirada do objeto continuará a permanecer no sistema de arquivos se a versão tiver sido capturada como uma versão atual em um ou mais snapshots S3. Essa versão do objeto deixará de existir no sistema de arquivos somente quando esse snapshot for excluído.

Da mesma forma, em um intervalo no qual o controle de versão é desativado, se um objeto é excluído com base em uma regra de expiração, mas o objeto ainda é capturado em alguns snapshots S3 existentes, o objeto será retido no sistema de arquivos. O objeto será removido permanentemente do sistema de arquivos quando os snapshots que capturam forem excluídos.

Para obter informações sobre a expiração do objeto S3 e o gerenciamento do ciclo de vida, "Crie uma regra de gerenciamento do ciclo de vida do bucket"consulte .

Limitações com S3 instantâneos

Observe as seguintes exclusões e cenários de recursos no ONTAP 9.16,1:

- Você pode gerar até 1023 snapshots para um bucket do S3.

- É necessário excluir todos os snapshots e metadados do S3 de todos os buckets em um cluster antes de reverter o cluster para uma versão do ONTAP anterior ao ONTAP 9.16,1.
- Se você precisar excluir um bucket do S3 contendo objetos com snapshots, verifique se você excluiu todos os snapshots correspondentes de todos os objetos nesse bucket.
- S3 snapshots não são suportados nessas configurações:
  - Em buckets em um relacionamento com o SnapMirror
  - Em buckets onde o bloqueio de objetos está ativado
  - No NetApp BlueXP
  - No System Manager
  - Nas configurações do ONTAP MetroCluster

Crie instantâneos S3D.

Você pode gerar snapshots S3 manualmente ou configurar políticas de snapshot para criar snapshots S3 automaticamente para você. Os snapshots servem como cópias estáticas de objetos que você usa para backup e recuperação de dados. Para determinar a duração da retenção de snapshot, você pode criar políticas de snapshot que facilitem a criação automática de snapshot em intervalos especificados.

Os snapshots S3 ajudam a proteger os dados de objetos em buckets do S3 com ou sem o controle de versão de objetos ativado.

Os snapshots podem ser especialmente úteis no estabelecimento da proteção de dados quando o controle de versão de objetos não está habilitado em um bucket do S3, porque atuam como Registros pontuais que podem ser usados para operações de restauração quando uma versão de objeto anterior não está disponível.

Sobre esta tarefa

- As seguintes regras de nomenclatura aplicam-se ao instantâneo (para instantâneos manuais e automáticos):
  - Os nomes de instantâneos S3 podem ter até 30 carateres
  - S3 os nomes de instantâneos podem consistir apenas em letras minúsculas, números, pontos (.) e hífens (-)
  - Os nomes de instantâneos S3 devem terminar com uma letra ou um número
  - Os nomes de instantâneos S3 não podem conter subcadeia de carateres `s3snap`
- No contexto do protocolo S3, as restrições de nomes de buckets limitam um nome de bucket a 63 carateres. Como os snapshots do ONTAP S3 são apresentados como buckets por meio do protocolo S3, restrições semelhantes se aplicam aos nomes dos buckets do snapshot. Por padrão, o nome do bucket original é usado como o nome do bucket base.
- Para facilitar a identificação de qual snapshot pertence a qual bucket, o nome do bucket do snapshot consiste no nome do bucket base, juntamente com uma string especial, `-s3snap-` que é prefixada ao nome do snapshot. Os nomes do bucket do instantâneo são formatados como `<base_bucket_name>-s3snap-<snapshot_name>`.

  Por exemplo, executar o comando a seguir para criar `snap1` no `bucket-a` cria um bucket de snapshot com nome `bucket-a-s3snap-snap1`, que pode ser acessado por meio de clientes S3 se você tiver

permissões para acessar o bucket base.

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- Não é possível criar um instantâneo que resulte em um nome de intervalo de instantâneo com mais de 63 carateres.
- O nome do instantâneo automático contém o nome do agendamento da política e o carimbo de data/hora, que é semelhante à convenção de nomenclatura para os instantâneos de volume tradicionais. Por exemplo, os nomes de instantâneos programados podem ser `daily-2024-01-01-0015` e `hourly-2024-05-22-1105`.

Crie manualmente S3 instantâneos

Você pode criar manualmente um snapshot S3 usando a CLI do ONTAP. O procedimento cria um instantâneo apenas no cluster local.

Passos

1. Criar um instantâneo S3D:

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

O exemplo a seguir cria um snapshot nomeado `pre-update` na `vs0` VM e bucket do storage `website-data`:

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

Atribua uma política de snapshot S3 a um bucket

Quando você configura políticas de snapshot no nível do bucket do S3, o ONTAP cria snapshots S3 programados para você automaticamente. Como as políticas de snapshot tradicionais, até cinco programações podem ser configuradas para snapshots S3.

Uma política de snapshot normalmente especifica as agendas para criar snapshots, o número de cópias a reter para cada agendamento e o prefixo de agendamento. Por exemplo, uma política pode criar um snapshot S3 todos os dias às 12:10 AM, reter as duas cópias mais recentes e nomeá-las `daily-<timestamp>`.

A política de snapshot padrão preserva:

- Seis snapshots por hora
- Dois instantâneos diários
- Dois instantâneos semanais

Antes de começar

- Uma política de snapshot deve ter sido criada antes de atribuí-la ao bucket S3.

> As políticas para snapshots S3 seguem as mesmas regras que outras políticas de snapshot do ONTAP. No entanto, uma política de snapshot com um período de retenção configurado em qualquer uma das programações de snapshot não pode ser atribuída a um bucket do S3.

Para obter mais informações sobre a criação de políticas de snapshot para geração automática de snapshots, "Configure a visão geral das políticas de snapshot personalizadas"consulte .

Passos

1. Atribua a política de snapshot no bucket:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

ou

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

> Se for necessário reverter um cluster para uma versão do ONTAP anterior ao ONTAP 9.16,1, verifique se o valor para `snapshot-policy` todos os buckets está definido como `none` (ou `-`).

Informações relacionadas

"Visão geral do instantâneo do S3"

Visualizar e restaurar snapshots S3

O recurso de snapshot do ONTAP S3 permite exibir e navegar o conteúdo de snapshot do S3 para seus buckets de clientes do S3. Além disso, você pode restaurar um único objeto, um conjunto de objetos ou um bucket inteiro em um cliente S3 a partir de um snapshot S3.

Antes de começar

Para visualizar, navegar e restaurar instantâneos do ONTAP S3 nos seus buckets, os instantâneos devem ter sido criados e o bucket base do S3 deve estar acessível a você por meio do cliente de protocolo S3.

Liste e e visualize instantâneos S3D.

Você pode visualizar os detalhes do snapshot do S3, compará-los e identificar erros. Usando a CLI do ONTAP, você pode listar todos os snapshots criados nos buckets do S3.

Passos

1. Listar S3 instantâneos:

```
vserver object-store-server bucket snapshot show
```

É possível visualizar os nomes dos snapshots, as VMs de storage, os buckets, o tempo de criação e `instance-uuid` os snapshots do S3 criados para todos os buckets no cluster.

2. Você também pode especificar um nome de bucket para exibir os nomes, o tempo de criação e `instance-uuid` todos os snapshots S3 criados para esse bucket específico.

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

PESQUISE conteúdo de instantâneos S3

Se você notar falhas ou problemas no seu ambiente, poderá navegar pelo conteúdo dos snapshots do bucket do S3 para identificar os erros. Você também pode navegar nos snapshots S3 para determinar o conteúdo livre de erros a ser restaurado.

Os snapshots S3 são apresentados como buckets de snapshot para os clientes S3. O nome do bucket do instantâneo é formatado como `<base_bucket_name>-s3snap-<snapshot_name>`. Você pode ver todos os buckets de snapshot em uma VM de storage usando a `ListBuckets` operação da API S3.

O bucket do snapshot S3 herda as políticas de acesso do bucket base e dá suporte apenas a operações somente leitura. Se você tiver permissões para acessar o bucket base, também poderá executar operações de API S3D somente leitura no bucket do snapshot S3, como `HeadObject` `GetObject` , , `GetObjectTagging` `ListObjects` , , , `ListObjectVersions`, `GetObjectAcl`, e `CopyObject`.

> ⓘ A `CopyObject` operação é suportada em um bucket de instantâneos do S3 somente se for uma cópia instantânea do bucket de origem, e não se for o destino de armazenamento do snapshot.

Para obter mais informações sobre essas operações, "Ações compatíveis com o ONTAP S3"consulte .

Restaure o conteúdo de snapshots S3

Você pode executar uma operação de restauração em um cliente S3 para recuperar um único objeto, um conjunto de objetos ou um bucket inteiro copiando o conteúdo de um bucket de snapshot para o bucket original ou diferente. Você pode procurar instantâneos para determinar qual conteúdo de snapshot você deve copiar.

Você restaura todo o bucket, objetos com um prefixo ou um único objeto usando o `aws s3 cp` comando.

Passos

1. Tire um instantâneo do balde base S3.

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. Restaure o bucket da base usando o snapshot:
   - Restaure um balde inteiro. Use o nome do bucket do instantâneo no formato `<base_bucket_name>-s3snap-<snapshot_name>`.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

   - Restaure objetos em um diretório com o prefixo `dir1`:

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

   - Restaurar um único objeto chamado `web.py`:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

Eliminar S3 instantâneos

Você pode excluir snapshots S3 que não precisam mais e liberar espaço de armazenamento em seus buckets. Você pode remover manualmente snapshots S3 ou modificar as políticas de snapshot anexadas aos buckets do S3 para alterar o número de snapshots a serem retidos para um agendamento.

As políticas de snapshot para buckets do S3 seguem as mesmas regras de exclusão das políticas tradicionais de snapshot do ONTAP. Para obter mais informações sobre como criar políticas de snapshot, "Criar uma política de snapshot"consulte .

Sobre esta tarefa

- Se uma versão de objeto (em um bucket versionado) ou um objeto (em um bucket não versionado) for capturada em vários snapshots, o objeto será removido do sistema de arquivos somente após o último snapshot protegendo-o ser excluído.
- Se você precisar excluir um bucket do S3 contendo objetos com snapshots, verifique se você excluiu todos os snapshots de todos os objetos nesse bucket.
- Se você precisar reverter um cluster para uma versão do ONTAP anterior ao ONTAP 9.16,1, certifique-se de excluir todos os snapshots do S3 para todos os buckets. Você também pode precisar executar o `vserver object-store-server bucket clear-snapshot-metadata` comando para remover os metadados de snapshot de um bucket do S3. Para obter informações, "Limpar metadados de instantâneos do S3"consulte .
- Ao excluir snapshots em lotes, você pode remover um grande número de objetos capturados em vários snapshots, liberando efetivamente mais espaço do que a exclusão individual de snapshot causaria. Como resultado, você pode recuperar mais espaço para seus objetos de storage.

Passos

1. Para excluir um snapshot S3 específico, execute este comando:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. Para remover todos os snapshots S3 em um bucket, execute este comando:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

Limpar metadados de instantâneos do S3

Com snapshots S3, os metadados de snapshot também são gerados em um bucket. Os metadados do snapshot continuam a estar no bucket, mesmo que todos os snapshots sejam removidos dele. A presença de metadados do Snapshot bloqueia as seguintes operações:

- O cluster reverte para uma versão do ONTAP anterior ao ONTAP 9.16,1
- Configuração do SnapMirror S3 no balde

Antes de executar essas operações, você deve limpar todos os metadados do snapshot do bucket.

Antes de começar

Certifique-se de que removeu todos os instantâneos do S3 de um intervalo antes de começar a limpar os metadados.

Passos

1. Para limpar os metadados de snapshot de um bucket, execute este comando:

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

Auditoria S3 eventos

Auditoria S3 eventos

A partir do ONTAP 9.10,1, você pode auditar dados e eventos de gerenciamento em ambientes ONTAP S3. A funcionalidade de auditoria do S3 é semelhante aos recursos de auditoria nas existentes, e a auditoria do S3 e nas pode coexistir em um cluster.

Quando você cria e ativa uma configuração de auditoria do S3 em um SVM, os eventos do S3 são registrados em um arquivo de log. Você pode especificar os seguintes eventos a serem registrados:

Eventos de acesso a objetos (dados) por lançamento

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects of 9.10.1 foi renomeado para este)
- ListAllMyBuckets (ListBuckets de 9.10.1 foi renomeado para este)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPCompletar
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- Marcação de objetos
- ListUploads
- ListParts

Eventos de gerenciamento por liberação

9.15.1:

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- Retenção PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- Política de GetBucketPolicy
- CopyObject
- UploadPartCopy
- Política de PutBucketPolicy
- DeleteBucketPolicy

9.11.1:

- GetBucketControle de versão
- PutBucketControle de versão

9.10.1:

- Balde para a cabeça
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketlocalização

O formato de log é JavaScript Object Notation (JSON).

O limite combinado para configurações de auditoria S3 e NFS é de 50 SVMs por cluster.

É necessária a seguinte licença:

- ONTAP One, anteriormente parte do pacote principal, para protocolo e storage ONTAP S3

Para obter mais informações, "Como funciona o processo de auditoria do ONTAP"consulte .

Auditoria garantida

Por padrão, a auditoria S3 e nas é garantida. O ONTAP garante que todos os eventos de acesso de bucket auditáveis sejam registrados, mesmo que um nó não esteja disponível. Uma operação de bucket solicitada não pode ser concluída até que o Registro de auditoria dessa operação seja salvo no volume de estadiamento no armazenamento persistente. Se os Registros de auditoria não puderem ser confirmados nos arquivos de teste, seja por espaço insuficiente ou por causa de outros problemas, as operações do cliente serão negadas.

Requisitos de espaço para auditoria

No sistema de auditoria do ONTAP, os Registros de auditoria são armazenados inicialmente em arquivos de teste binário em nós individuais. Periodicamente, eles são consolidados e convertidos em logs de eventos legíveis pelo usuário, que são armazenados no diretório de log de eventos de auditoria do SVM.

Os arquivos de estadiamento são armazenados em um volume de estadiamento dedicado, que é criado pelo ONTAP quando a configuração de auditoria é criada. Há um volume de estadiamento por agregado.

Você precisa Planejar espaço disponível suficiente na configuração de auditoria:

- Para os volumes de estadiamento em agregados que contêm buckets auditados.
- Para o volume que contém o diretório onde os logs de eventos convertidos são armazenados.

Você pode controlar o número de logs de eventos e, portanto, o espaço disponível no volume, usando um de dois métodos ao criar a configuração de auditoria S3:

- Um limite numérico; o `-rotate-limit` parâmetro controla o número mínimo de arquivos de auditoria que devem ser preservados.
- Um limite de tempo; o `-retention-duration` parâmetro controla o período máximo que os arquivos podem ser preservados.

Em ambos os parâmetros, uma vez que o configurado é excedido, os arquivos de auditoria mais antigos podem ser excluídos para abrir espaço para os mais novos. Para ambos os parâmetros, o valor é 0, indicando que todos os arquivos devem ser mantidos. Para garantir espaço suficiente, é, portanto, uma prática recomendada definir um dos parâmetros para um valor não zero.

Devido à auditoria garantida, se o espaço disponível para os dados de auditoria acabar antes do limite de rotação, os dados de auditoria mais recentes não podem ser criados, resultando em falha no acesso dos clientes aos dados. Portanto, a escolha desse valor e do espaço alocado à auditoria deve ser escolhida cuidadosamente, e você deve responder a avisos sobre o espaço disponível do sistema de auditoria.

Para obter mais informações, "Conceitos básicos de auditoria"consulte .

Planejar uma configuração de auditoria S3

Você deve especificar vários parâmetros para a configuração de auditoria S3 ou aceitar os padrões. Em particular, você deve considerar quais parâmetros de rotação de log ajudarão a garantir espaço livre adequado.

Consulte a *`vserver object-store-server audit create`página man * para obter detalhes de sintaxe.

Parâmetros gerais

Há dois parâmetros necessários que você deve especificar ao criar a configuração de auditoria. Há também três parâmetros opcionais que você pode especificar.

Tipo de informação	Opção	Obrigatório
Nome da SVM Nome do SVM no qual você pode criar a configuração de auditoria. O SVM já deve existir e estar habilitado para S3.	`-vserver` *`svm_name`*	Sim

Log Destination path Especifica onde os logs de auditoria convertidos são armazenados. O caminho já deve existir no SVM. O caminho pode ter até 864 carateres de comprimento e deve ter permissões de leitura e gravação. Se o caminho não for válido, o comando de configuração de auditoria falhará.	`-destination` *text*	Sim
Categorias de eventos a auditar As seguintes categorias de eventos podem ser auditadas: • Eventos GetObject, PutObject e DeleteObject de dados • Eventos PutBucket de Gestão e DeleteBucket O padrão é auditar somente eventos de dados.	`-events {data|management}, …`	Não

Pode introduzir um dos seguintes parâmetros para controlar o número de ficheiros de registo de auditoria. Se nenhum valor for inserido, todos os arquivos de log serão retidos.

Tipo de informação	Opção	Obrigatório
Limite de rotação de arquivos de log Determina quantos arquivos de log de auditoria devem ser mantidos antes de girar o arquivo de log mais antigo. Por exemplo, se você inserir um valor de 5, os últimos cinco arquivos de log serão retidos. Um valor de 0 indica que todos os arquivos de log são mantidos. O valor padrão é 0.	`-rotate-limit` *integer*	Não
Limite de duração dos ficheiros de registo Determina por quanto tempo um arquivo de log pode ser retido antes de ser excluído. Por exemplo, se você inserir um valor de 5d0h0m, os logs com mais de 5 dias serão excluídos. Um valor de 0 indica que todos os arquivos de log são mantidos. O valor padrão é 0.	`-retention duration` *integer_time*	Não

Parâmetros para rotação do log de auditoria

Você pode girar os logs de auditoria com base no tamanho ou na programação. O padrão é girar os logs de auditoria com base no tamanho.

Rode registos com base no tamanho do registo

Se você quiser usar o método de rotação de log padrão e o tamanho padrão do log, não será necessário configurar nenhum parâmetro específico para a rotação de log. O tamanho padrão do log é de 100 MB.

Se você não quiser usar o tamanho padrão do log, você pode configurar o `-rotate-size` parâmetro para especificar um tamanho de log personalizado.

Se você quiser redefinir a rotação com base em um tamanho de log sozinho, use o seguinte comando para desdefinir o `-rotate-schedule-minute` parâmetro:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Gire os logs com base em um agendamento

Se você optar por girar os logs de auditoria com base em um agendamento, poderá agendar a rotação de logs usando os parâmetros de rotação baseados em tempo em qualquer combinação.

- Se utilizar rotação baseada no tempo, o `-rotate-schedule-minute` parâmetro é obrigatório.
- Todos os outros parâmetros de rotação baseados no tempo são opcionais.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- O programa de rotação é calculado utilizando todos os valores relacionados com o tempo. Por exemplo, se você especificar apenas o `-rotate-schedule-minute` parâmetro, os arquivos de log de auditoria serão girados com base nos minutos especificados em todos os dias da semana, durante todas as horas em todos os meses do ano.
- Se você especificar apenas um ou dois parâmetros de rotação baseados no tempo (por exemplo, `-rotate-schedule-month` e `-rotate-schedule-minutes`), os arquivos de log serão girados com base nos valores de minuto especificados em todos os dias da semana, durante todas as horas, mas somente durante os meses especificados.

  Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro, março e agosto em todas as segundas, quartas e sábados às 10:30 da manhã

- Se você especificar valores para ambos `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, eles serão considerados independentemente.

  Por exemplo, se você especificar `-rotate-schedule-dayofweek` como sexta-feira e `-rotate -schedule-day` como 13, os logs de auditoria serão girados em todas as sextas-feiras e no dia 13th do mês especificado, não apenas em todas as sextas-feiras, dia 13th.

- Se quiser redefinir a rotação com base em um agendamento sozinho, use o seguinte comando para desmarcar o `-rotate-size parameter`:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Rode registos com base no tamanho e na programação do registo

Você pode optar por girar os arquivos de log com base no tamanho do log e em uma programação, definindo o parâmetro -Rotate-size e os parâmetros de rotação baseados no tempo em qualquer combinação. Por exemplo: Se `-rotate-size` estiver definido para 10 MB e `-rotate-schedule-minute` estiver definido para 15, os arquivos de log rodam quando o tamanho do arquivo de log atinge 10 MB ou nos 15th minutos de cada hora (o que ocorrer primeiro).

Crie e habilite uma configuração de auditoria S3

Para implementar a auditoria do S3, primeiro você cria uma configuração de auditoria de armazenamento de objetos persistente em um SVM habilitado para S3 e, em seguida, ativa a configuração.

O que você vai precisar

- SVM habilitado para S3.
- Espaço suficiente para estadiamento de volumes no agregado.

Sobre esta tarefa

É necessária uma configuração de auditoria para cada SVM que contenha buckets do S3 que você deseja auditar. Você pode habilitar a auditoria S3 em servidores S3 novos ou existentes. As configurações de auditoria persistem em um ambiente S3 até serem removidas pelo comando **vserver object-store-server audit delete**.

A configuração de auditoria do S3 se aplica a todos os buckets do SVM que você selecionar para auditoria. Um SVM habilitado para auditoria pode conter buckets auditados e não auditados.

É recomendável configurar a auditoria S3 para rotação automática de logs, determinada pelo tamanho do log ou por um agendamento. Se você não configurar a rotação automática de log, todos os arquivos de log serão retidos por padrão. Você também pode girar arquivos de log S3 manualmente usando o comando **vserver object-store-server audit rotate-log**.

Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino não poderá estar no volume raiz.

Procedimento

1. Crie a configuração de auditoria para girar logs de auditoria com base no tamanho do log ou em uma programação.

Se você quiser girar logs de auditoria…	Digite…
Tamanho do registo	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integer_d][_integer_h][_integer_m][_integers`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`

Se você quiser girar logs de auditoria…	Digite…
Uma programação	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integerd`*`][`*`integerh`*`] [`*`integerm`*`][`*`integers`*`]] } [-rotate-schedule-month` *`chron_month`*`] [-rotate-schedule-dayofweek` *`chron_dayofweek`*`] [-rotate-schedule-day` *`chron_dayofmonth`*`] [-rotate-schedule-hour` *`chron_hour`*`] -rotate-schedule-minute` *`chron_minute`* O `-rotate-schedule-minute` parâmetro é necessário se você estiver configurando a rotação de log de auditoria baseada em tempo.

2. Ativar auditoria S3:

   `vserver object-store-server audit enable -vserver` *`svm_name`*

Exemplos

O exemplo a seguir cria uma configuração de auditoria que audita todos os eventos S3 (o padrão) usando rotação baseada em tamanho. Os logs são armazenados no diretório /audit_log. O limite de tamanho do arquivo de log é de 200 MB. Os logs são girados quando atingem 200 MB de tamanho.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

O exemplo a seguir cria uma configuração de auditoria que audita todos os eventos S3 (o padrão) usando rotação baseada em tamanho. O limite de tamanho do arquivo de log é de 100 MB (o padrão) e os logs são mantidos por 5 dias antes de serem excluídos.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

O exemplo a seguir cria uma configuração de auditoria que audita eventos de gerenciamento S3 e eventos de preparação de políticas de acesso central usando rotação baseada em tempo. Os logs de auditoria são girados mensalmente, às 12:30 horas em todos os dias da semana. O limite de rotação do registo é 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Selecione buckets para auditoria S3

Você precisa especificar quais buckets auditar em um SVM habilitado para auditoria.

O que você vai precisar

- Um SVM foi habilitado para auditoria S3.

Sobre esta tarefa

As configurações de auditoria do S3 são habilitadas por SVM, mas você precisa selecionar os buckets no SVMS que estão habilitados para auditoria. Se você adicionar buckets ao SVM e quiser que os novos buckets sejam auditados, selecione-os com este procedimento. Também é possível ter buckets não auditados em uma SVM habilitada para auditoria S3.

As configurações de auditoria persistem para buckets até serem removidas pelo `vserver object-store-server audit event-selector delete` comando.

Procedimento

Selecione um bucket para a auditoria S3:

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

- `-access` - especifica o tipo de acesso a eventos a ser auditado: `read-only`, `write-only` ou `all` (o padrão é `all`).
- `-permission` - especifica o tipo de permissão de evento a ser auditado: `allow-only`, `deny-only` ou `all` (o padrão é `all`).

Exemplo

O exemplo a seguir cria uma configuração de auditoria de bucket que somente Registra eventos permitidos com acesso somente leitura:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Modificar uma configuração de auditoria S3

É possível modificar os parâmetros de auditoria de buckets individuais ou a configuração de auditoria de todos os buckets selecionados para auditoria no SVM.

Se você quiser modificar a configuração de auditoria para…	Digite…
Baldes individuais	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
Todos os buckets no SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Exemplos

O exemplo a seguir modifica uma configuração de auditoria de bucket individual para auditar somente eventos de acesso somente gravação:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

O exemplo a seguir modifica a configuração de auditoria de todos os buckets no SVM para alterar o limite de tamanho do log para 10MB e reter arquivos de log 3 antes de girar.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Mostrar configurações de auditoria do S3

Depois de concluir a configuração de auditoria, você pode verificar se a auditoria está configurada corretamente e está habilitada. Você também pode exibir informações sobre todas as configurações de auditoria de armazenamento de objetos no cluster.

Sobre esta tarefa

É possível exibir informações sobre configurações de auditoria de bucket e SVM.

- Buckets – use o `vserver object-store-server audit event-selector show` comando

  Sem parâmetros, o comando exibe as seguintes informações sobre buckets em todos os SVMs no cluster com configurações de auditoria de armazenamento de objetos:

  - Nome do SVM
  - Nome do intervalo
  - Valores de acesso e permissão
- SVMs – use o `vserver object-store-server audit show` comando

  Sem parâmetros, o comando exibe as seguintes informações sobre todos os SVMs no cluster com configurações de auditoria de armazenamento de objetos:

  - Nome do SVM
  - Estado de auditoria
  - Diretório de destino

Você pode especificar o `-fields` parâmetro para especificar quais informações de configuração de auditoria serão exibidas.

Procedimento

Mostrar informações sobre configurações de auditoria do S3:

Se pretender modificar a configuração para…	Digite…
Baldes	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Se pretender modificar a configuração para…	Digite…
SVMs	`vserver object-store-server audit show [-vserver` *svm_name*`] [`*parameters*`]`

Exemplos

O exemplo a seguir exibe informações para um único bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

O exemplo a seguir exibe informações de todos os buckets em um SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

O exemplo a seguir exibe o nome, o estado de auditoria, os tipos de eventos, o formato de log e o diretório de destino para todos os SVMs.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

O exemplo a seguir exibe os nomes e detalhes da SVM sobre o log de auditoria de todos os SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details

                Rotation                            Rotation
      Vserver   File Size Rotation Schedule         Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                        0
```

O exemplo a seguir exibe em forma de lista todas as informações de configuração de auditoria sobre todos os SVMs.

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                           Log Format: json
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
                   Log Retention Time: 0s
```

Autenticação e controle de acesso

Visão geral do controle de acesso e autenticação

Você pode gerenciar a autenticação de cluster do ONTAP e o controle de acesso aos serviços da Web do ONTAP.

Com o System Manager ou a CLI, você pode controlar e proteger o acesso do cliente e do administrador ao cluster e ao storage.

Se você estiver usando o Gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e anterior), consulte "System Manager Classic (ONTAP 9 9,7.0 a 0)"

Autenticação e autorização do cliente

O ONTAP autentica uma máquina cliente e um usuário verificando suas identidades com uma fonte confiável. O ONTAP autoriza um usuário a acessar um arquivo ou diretório comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório.

Autenticação de administrador e RBAC

Os administradores usam contas de login locais ou remotas para se autenticar no cluster e na VM de armazenamento. O controle de acesso baseado em função (RBAC) determina os comandos aos quais um administrador tem acesso.

Gerenciar a autenticação do administrador e o RBAC

Visão geral da autenticação do administrador e do RBAC com a CLI

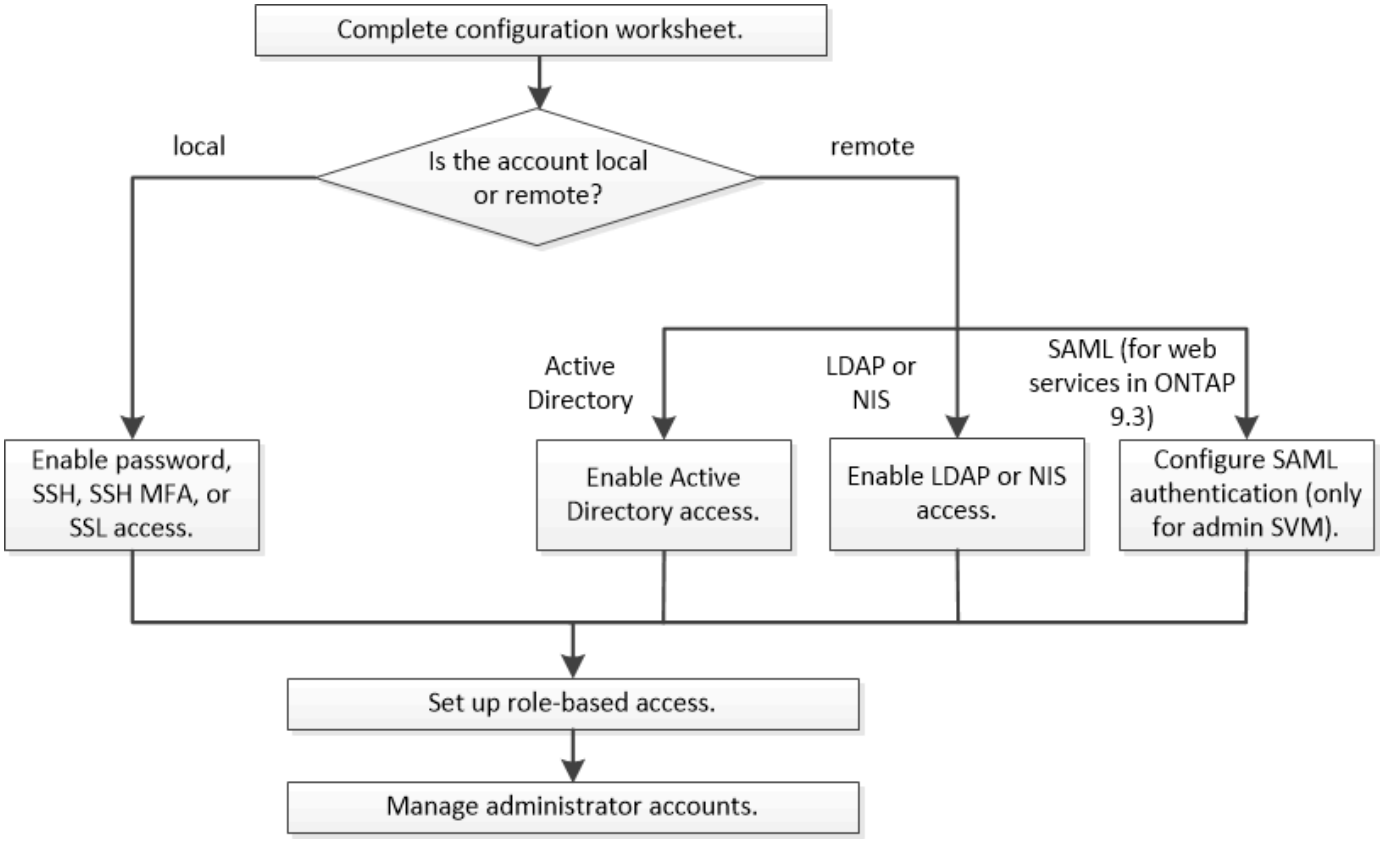
Você pode habilitar contas de login para administradores de cluster do ONTAP e administradores de máquina virtual de storage (SVM). Você também pode usar o controle de acesso baseado em função (RBAC) para definir as funcionalidades dos administradores.

Você ativa as contas de login e o RBAC das seguintes maneiras:

- Você deseja usar a interface de linha de comando (CLI) do ONTAP, não o Gerenciador de sistema ou uma ferramenta de script automatizado.
- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você não está usando SNMP para coletar informações sobre o cluster.

Autenticação de administrador e fluxo de trabalho RBAC

Você pode ativar a autenticação para contas de administrador locais ou contas de administrador remoto. As informações da conta de uma conta local residem no sistema de armazenamento e as informações da conta de uma conta remota residem em outro lugar. Cada conta pode ter uma função predefinida ou uma função personalizada.



Você pode habilitar contas de administrador locais para acessar uma máquina virtual de storage de administrador (SVM) ou um data SVM com os seguintes tipos de autenticação:

- Palavra-passe
- Chave pública SSH
- Certificado SSL
- Autenticação multifator SSH (MFA)

  A partir do ONTAP 9.3, a autenticação com senha e chave pública é suportada.

Você pode habilitar contas de administrador remoto para acessar um SVM admin ou um SVM de dados com os seguintes tipos de autenticação:

- Ative Directory
- Autenticação SAML (somente para SVM de administrador)

  A partir do ONTAP 9.3, a autenticação SAML (Security Assertion Markup Language) pode ser usada para acessar o SVM admin usando qualquer um dos seguintes serviços da Web: Infraestrutura do processador de serviços, APIs ONTAP ou Gerenciador de sistemas.

- A partir do ONTAP 9.4, o SSH MFA pode ser usado para usuários remotos em servidores LDAP ou NIS. A autenticação com nsswitch e chave pública é suportada.

Planilhas para autenticação de administrador e configuração RBAC

Antes de criar contas de login e configurar o controle de acesso baseado em funções (RBAC), você deve coletar informações para cada item nas planilhas de configuração.

Criar ou modificar contas de login

Você fornece esses valores com o `security login create` comando ao habilitar contas de login para acessar uma VM de armazenamento. Você fornece os mesmos valores com o `security login modify` comando quando modifica como uma conta acessa uma VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento que a conta acessa. O valor padrão é o nome da VM de armazenamento de administrador para o cluster.	
`-user-or-group-name`	O nome de usuário ou nome de grupo da conta. Especificar um nome de grupo permite o acesso a cada usuário no grupo. Você pode associar um nome de usuário ou nome de grupo a vários aplicativos.	
`-application`	O aplicativo usado para acessar a VM de storage: • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	O método utilizado para autenticar a conta: • `cert` Para autenticação de certificado SSL • `domain` Para autenticação do ative Directory • `nsswitch` Para autenticação LDAP ou NIS • `password` para autenticação de senha do usuário • `publickey` para autenticação de chave pública • `community` Para strings de comunidade SNMP • `usm` Para o modelo de segurança do utilizador SNMP • `saml` Para autenticação SAML (Security Assertion Markup Language)	
`-remote-switch-ipaddress`	O endereço IP do interrutor remoto. O switch remoto pode ser um switch de cluster monitorado pelo monitor de integridade do switch de cluster (CSHM) ou um switch Fibre Channel (FC) monitorado pelo monitor de integridade do MetroCluster (MCC-HM). Esta opção é aplicável apenas quando a aplicação é `snmp` e o método de autenticação é `usm`.	
`-role`	A função de controle de acesso atribuída à conta: • Para o cluster (a VM de armazenamento de administrador), o valor padrão é `admin`. • Para uma VM de armazenamento de dados, o valor padrão é `vsadmin`.	
`-comment`	(Opcional) texto descritivo para a conta. Você deve incluir o texto entre aspas duplas (").	

`-is-ns-switch-group`	Se a conta é uma conta de grupo LDAP ou uma conta de grupo NIS (`yes` ou `no`).	
`-second-authentication-method`	Segundo método de autenticação no caso de autenticação multifator: • `none` se não estiver usando autenticação multifator, o valor padrão • `publickey` para autenticação de chave pública quando o `authmethod` é senha ou nsswitch • `password` para autenticação de senha do usuário quando a `authmethod` é chave pública • `nsswitch` para autenticação de senha do usuário quando o authmethod é publikey A ordem de autenticação é sempre a chave pública seguida pela senha.	
`-is-ldap-fastbind`	A partir do ONTAP 9.11,1, quando definido como verdadeiro, ativa a vinculação rápida LDAP para autenticação nsswitch; o padrão é falso. Para utilizar a ligação rápida LDAP, o `-authentication-method` valor tem de ser definido como `nsswitch`. "Saiba mais sobre LDAP fastbind para autenticação nsswitch."	

Configure as informações de segurança do Cisco Duo

Você fornece esses valores com o `security login duo create` comando quando ativa a autenticação de dois fatores do Cisco Duo com logins SSH para uma VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	A VM de armazenamento (referida como vserver na CLI do ONTAP) à qual as configurações de autenticação Duo se aplicam.	

`-integration-key`	Sua chave de integração, obtida ao Registrar seu aplicativo SSH com Duo.	
`-secret-key`	Sua chave secreta, obtida ao Registrar seu aplicativo SSH com Duo.	
`-api-host`	O nome de host da API, obtido ao Registrar seu aplicativo SSH com Duo. Por exemplo: `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Em erros de serviço ou configuração que impedem a autenticação Duo, `safe` falha (permitir acesso) ou `secure` (negar acesso). O padrão é `safe`, o que significa que a autenticação Duo é ignorada se falhar devido a erros como o servidor de API Duo ficar inacessível.	
`-http-proxy`	Use o proxy HTTP especificado. Se o proxy HTTP exigir autenticação, inclua as credenciais no URL do proxy. Por exemplo: `http-proxy=http://username:password@proxy.example.org:8080`	

-autopush	`true` `false`Ou . A predefinição é `false`. Se `true`o , o Duo enviar automaticamente uma solicitação de login por push para o telefone do usuário, revertendo para uma chamada telefônica se o push não estiver disponível. Observe que isso desabilita efetivamente a autenticação por senha. Se `false`, o usuário for solicitado a escolher um método de autenticação. Quando configurado com `autopush = true`, recomendamos a configuração `max-prompts = 1`.	

`-max-prompts`	Se um usuário não conseguir autenticar com um segundo fator, o Duo solicitará que ele se autentique novamente. Esta opção define o número máximo de prompts que o Duo exibe antes de negar acesso. Deve ser `1`, `2`, `3` ou . O valor padrão é `1`. Por exemplo, quando `max-prompts = 1`o , o usuário precisa se autenticar com êxito no primeiro prompt, enquanto se , se `max-prompts = 2` o usuário inserir informações incorretas no prompt inicial, ele será solicitado a autenticar novamente. Quando configurado com `autopush = true`, recomendamos a configuração `max-prompts = 1`. Para obter a melhor experiência, um usuário com apenas autenticação publickey sempre terá `max-prompts` definido como `1`.	
`-enabled`	Ative a autenticação de dois fatores Duo. Defina como `true` por padrão. Quando ativada, a autenticação de dois fatores Duo é aplicada durante o login SSH de acordo com os parâmetros configurados. Quando Duo está desativado (definido para `false`), a autenticação Duo é ignorada.	
`-pushinfo`	Esta opção fornece informações adicionais na notificação push, como o nome do aplicativo ou serviço que está sendo acessado. Isso ajuda os usuários a verificar se estão fazendo login no serviço correto e fornece uma camada adicional de segurança.	

Definir funções personalizadas

Você fornece esses valores com o `security login role create` comando quando define uma função personalizada.

Campo	Descrição	O seu valor
`-vserver`	(Opcional) o nome da VM de armazenamento (referida como vserver na CLI do ONTAP) que está associado à função.	
`-role`	O nome da função.	
`-cmddirname`	O diretório de comando ou comando ao qual a função dá acesso. Você deve incluir nomes de subdiretório de comando em aspas duplas ("). Por exemplo, `"volume snapshot"`. Você deve digitar `DEFAULT` para especificar todos os diretórios de comando.	
`-access`	(Opcional) o nível de acesso para a função. Para diretórios de comando: • `none` (o valor padrão para funções personalizadas) nega o acesso aos comandos no diretório de comandos • `readonly` concede acesso aos `show` comandos no diretório de comandos e seus subdiretórios • `all` concede acesso a todos os comandos no diretório de comandos e seus subdiretórios Para *comandos não intrínsecos* (comandos que não terminam em `create`, `modify`, , `delete` ou `show`): • `none` (o valor padrão para funções personalizadas) nega o acesso ao comando • `readonly` não é aplicável • `all` concede acesso ao comando Para conceder ou negar acesso a comandos intrínsecos, você deve especificar o diretório de comandos.	

`-query`	(Opcional) o objeto de consulta que é usado para filtrar o nível de acesso, que é especificado na forma de uma opção válida para o comando ou para um comando no diretório de comandos. Você deve incluir o objeto de consulta em aspas duplas ("). Por exemplo, se o diretório de comando for `volume`, o objeto query `"-aggr aggr0"` ativará o acesso somente para `aggr0` o agregado.	

Associar uma chave pública a uma conta de utilizador

Você fornece esses valores com o `security login publickey create` comando ao associar uma chave pública SSH a uma conta de usuário.

Campo	Descrição	O seu valor
`-vserver`	(Opcional) o nome da VM de armazenamento que a conta acessa.	
`-username`	O nome de utilizador da conta. O valor padrão, `admin`, que é o nome padrão do administrador do cluster.	
`-index`	O número de índice da chave pública. O valor padrão é 0 se a chave for a primeira chave criada para a conta; caso contrário, o valor padrão é mais um do que o número de índice mais alto existente para a conta.	
`-publickey`	A chave pública OpenSSH. Você deve incluir a chave entre aspas duplas (").	
`-role`	A função de controle de acesso atribuída à conta.	
`-comment`	(Opcional) texto descritivo para a chave pública. Você deve incluir o texto entre aspas duplas (").	

`-x509-certificate`	(Opcional) começando com ONTAP 9.13,1, permite gerenciar a associação de certificados X,509 com a chave pública SSH. Quando você associa um certificado X,509 à chave pública SSH, o ONTAP verifica o login SSH para ver se esse certificado é válido. Se tiver expirado ou tiver sido revogado, o início de sessão é proibido e a chave pública SSH associada está desativada. Valores possíveis: • `install`: Instale o certificado X,509 codificado PEM especificado e associe-o à chave pública SSH. Inclua o texto completo do certificado que deseja instalar. • `modify`: Atualize o certificado X,509 codificado PEM existente com o certificado especificado e associe-o à chave pública SSH. Inclua o texto completo do novo certificado. • `delete`: Remova a associação de certificado X,509 existente com a chave pública SSH.	

Configure as definições globais de autorização dinâmica

Começando com ONTAP 9.15,1, você fornece esses valores com o `security dynamic-authorization modify` comando. Para obter mais informações sobre a configuração de autorização dinâmica, "descrição geral da autorização dinâmica"consulte .

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a qual a configuração de pontuação de confiança deve ser modificada. Se você omitir esse parâmetro, a configuração de nível do cluster será usada.	

`-state`	O modo de autorização dinâmica. Valores possíveis: • `disabled`: (Predefinição) a autorização dinâmica está desativada. • `visibility`: Este modo é útil para testar a autorização dinâmica. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas, mas não aplicada. No entanto, qualquer atividade que tenha sido negada ou sujeita a desafios de autenticação adicionais é registrada. • `enforced`: Destinado a ser utilizado depois de ter concluído o teste com `visibility` o modo. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas e as restrições de atividade são aplicadas se as condições de restrição forem cumpridas. O intervalo de supressão também é aplicado, impedindo desafios de autenticação adicionais dentro do intervalo especificado.	
`-suppression-interval`	Impede desafios de autenticação adicionais dentro do intervalo especificado. O intervalo está no formato ISO-8601 e aceita valores de 1 minuto a 1 hora inclusive. Se definido como 0, o intervalo de supressão será desativado e o usuário sempre será solicitado a um desafio de autenticação, se for necessário.	
`-lower-challenge-boundary`	O limite inferior da porcentagem de desafio de autenticação multifator (MFA). O intervalo válido é de 0 a 99. O valor 100 é inválido, pois isso faz com que todas as solicitações sejam negadas. O valor padrão é 0.	

`-upper-challenge-boundary`	O limite superior da porcentagem de desafio do MFA. O intervalo válido é de 0 a 100. Isto deve ser igual ou superior ao valor do limite inferior. Um valor de 100 significa que cada solicitação será negada ou sujeita a um desafio de autenticação adicional; não há solicitações que sejam permitidas sem um desafio. O valor padrão é 90.	

Instale um certificado digital de servidor assinado pela CA

Você fornece esses valores com o `security certificate generate-csr` comando ao gerar uma solicitação de assinatura de certificado digital (CSR) para uso na autenticação de uma VM de armazenamento como um servidor SSL.

Campo	Descrição	O seu valor
`-common-name`	O nome do certificado, que é um nome de domínio totalmente qualificado (FQDN) ou um nome comum personalizado.	
`-size`	O número de bits na chave privada. Quanto maior o valor, mais segura a chave. O valor padrão é `2048`. Os valores possíveis são `512`, `1024`, `1536` `2048` e .	
`-country`	O país da VM de armazenamento, em um código de duas letras. O valor padrão é `US`. Consulte as páginas de manual para obter uma lista de códigos.	
`-state`	O estado ou a província da VM de armazenamento.	
`-locality`	A localidade da VM de armazenamento.	
`-organization`	A organização da VM de storage.	
`-unit`	A unidade na organização da VM de armazenamento.	

`-email-addr`	O endereço de e-mail do administrador do Contato para a VM de armazenamento.	
`-hash-function`	A função de hash criptográfico para assinar o certificado. O valor padrão é `SHA256`. Os valores possíveis são `SHA1`, `SHA256`, e `MD5`.	

Você fornece esses valores com o `security certificate install` comando ao instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou da VM de armazenamento como um servidor SSL. Apenas as opções relevantes para a configuração da conta são mostradas na tabela a seguir.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento na qual o certificado deve ser instalado.	
`-type`	O tipo de certificado: • `server` para certificados de servidor e certificados intermediários • `client-ca` Para o certificado de chave pública da CA raiz do cliente SSL • `server-ca` Para o certificado de chave pública da CA raiz do servidor SSL do qual o ONTAP é um cliente • `client` Para um certificado digital autoassinado ou CA-assinado e chave privada para o ONTAP como cliente SSL	

Configurar o acesso do controlador de domínio do ative Directory

Você fornece esses valores com o `security login domain-tunnel create` comando quando já configurou um servidor SMB para uma VM de armazenamento de dados e deseja configurar a VM de armazenamento como gateway ou *tunnel* para acesso ao controlador de domínio do ative Directory ao cluster.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a qual o servidor SMB foi configurado.	

Você fornece esses valores com o `vserver active-directory create` comando quando não configurou um servidor SMB e deseja criar uma conta de computador VM de armazenamento no domínio do ative Directory.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a qual você deseja criar uma conta de computador do ative Directory.	
`-account-name`	O nome NetBIOS da conta do computador.	
`-domain`	O nome de domínio totalmente qualificado (FQDN).	
`-ou`	A unidade organizacional no domínio. O valor padrão é `CN=Computers`. O ONTAP anexa esse valor ao nome de domínio para produzir o nome distinto do ative Directory.	

Configurar o acesso ao servidor LDAP ou NIS

Você fornece esses valores com o `vserver services name-service ldap client create` comando ao criar uma configuração de cliente LDAP para a VM de armazenamento.

Apenas as opções relevantes para a configuração da conta são mostradas na tabela a seguir:

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a configuração do cliente.	
`-client-config`	O nome da configuração do cliente.	
`-ldap-servers`	Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores LDAP aos quais o cliente se coneta.	
`-schema`	O esquema que o cliente usa para fazer consultas LDAP.	

`-use-start-tls`	Se o cliente usa Iniciar TLS para criptografar a comunicação com o servidor LDAP (`true`ou `false`). Iniciar TLS é compatível apenas para acesso a VMs de armazenamento de dados. Ele não é compatível com acesso a VMs de storage admin.	

Você fornece esses valores com o `vserver services name-service ldap create` comando ao associar uma configuração de cliente LDAP à VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento com a qual a configuração do cliente deve ser associada.	
`-client-config`	O nome da configuração do cliente.	
`-client-enabled`	Se a VM de armazenamento pode usar a configuração do cliente LDAP (`true`ou `false`).	

Você fornece esses valores com o `vserver services name-service nis-domain create` comando ao criar uma configuração de domínio NIS em uma VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento na qual a configuração do domínio deve ser criada.	
`-domain`	O nome do domínio.	
`-servers`	**ONTAP 9.0, 9,1**: Uma lista separada por vírgulas de endereços IP para os servidores NIS usados pela configuração do domínio.	

`-nis-servers`	Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores NIS que são usados pela configuração de domínio.	

Você fornece esses valores com o `vserver services name-service ns-switch create` comando quando especifica a ordem de pesquisa para fontes de serviço de nome.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento na qual a ordem de consulta do serviço de nomes deve ser configurada.	
`-database`	O banco de dados do serviço de nomes: • `hosts` Para ficheiros e serviços de nomes DNS • `group` Para arquivos, LDAP e serviços de nomes NIS • `passwd` Para arquivos, LDAP e serviços de nomes NIS • `netgroup` Para arquivos, LDAP e serviços de nomes NIS • `namemap` Para ficheiros e serviços de nomes LDAP	
`-sources`	A ordem pela qual procurar fontes do serviço de nomes (em uma lista separada por vírgulas): • `files` • `dns` • `ldap` • `nis`	

Configurar o acesso SAML

A partir do ONTAP 9.3, você fornece esses valores com o `security saml-sp create` comando para configurar a autenticação SAML.

Campo	Descrição	O seu valor

`-idp-uri`	O endereço FTP ou o endereço HTTP do host do provedor de identidade (IDP) de onde os metadados de IDP podem ser baixados.	
`-sp-host`	O nome do host ou o endereço IP do host do provedor de serviços SAML (sistema ONTAP). Por padrão, o endereço IP do LIF de gerenciamento de cluster é usado.	
`-cert-ca` e `-cert-serial`, ou `-cert-common-name`	Os detalhes do certificado do servidor do host do provedor de serviços (sistema ONTAP). Você pode inserir a autoridade de certificação de emissão de certificado do provedor de serviços (CA) e o número de série do certificado ou o Nome Comum do certificado do servidor.	
`-verify-metadata-server`	Se a identidade do servidor de metadados IDP deve ser validada `true` ou `false`). A melhor prática é sempre definir este valor para `true`.	

Criar contas de login

Criar uma visão geral das contas de login

Você pode habilitar contas de administrador de cluster local ou remoto e SVM. Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento. As informações da conta de ANÚNCIO são armazenadas em um controlador de domínio. As contas LDAP e NIS residem em servidores LDAP e NIS.

Administradores de clusters e SVM

Um *administrador de cluster* acessa o administrador SVM para o cluster. O administrador SVM e um administrador de cluster com o nome reservado `admin` são criados automaticamente quando o cluster é configurado.

Um administrador de cluster com a função padrão `admin` pode administrar todo o cluster e seus recursos. O administrador do cluster pode criar administradores de cluster adicionais com funções diferentes, conforme necessário.

Um *administrador do SVM* acessa um data SVM. O administrador do cluster cria SVMs de dados e administradores de SVM conforme necessário.

Por padrão, os administradores do SVM recebem `vsadmin` a função. O administrador do cluster pode atribuir funções diferentes aos administradores do SVM, conforme necessário.

Convenções de nomenclatura

Os seguintes nomes genéricos não podem ser usados para contas de administrador de cluster remoto e SVM:

- "adm"
- "bin" (caixa)
- "cli"
- "daemon"
- "ftp"
- "jogos"
- "parar"
- "lp"
- "correio"
- "homem"
- "naroot"
- "NetApp"
- "notícias"
- "ninguém"
- "operador"
- "raiz"
- "shutdown" (encerramento)
- "sshd"
- "sincronizar"
- "sys" (sistema)
- "uucp"
- "www"

Funções mescladas

Se você habilitar várias contas remotas para o mesmo usuário, será atribuída ao usuário a união de todas as funções especificadas para as contas. Ou seja, se uma conta LDAP ou NIS for atribuída à `vsadmin` função e a conta do grupo AD para o mesmo usuário for atribuída `vsadmin-volume` à função, o usuário do AD fará logon com os recursos mais inclusivos `vsadmin`. Diz-se que os papéis são *fundidos*.

Ative o acesso à conta local

Ative a visão geral do acesso à conta local

Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento. Você pode usar o `security login create` comando para habilitar contas locais para acessar um

administrador ou um SVM de dados.

Ativar acesso à conta de palavra-passe

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou data SVM com uma senha. Você será solicitado a digitar a senha depois de digitar o comando.

Sobre esta tarefa

Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Ative as contas de administrador locais para acessar um SVM usando uma senha:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir habilita a conta de administrador de cluster `admin1` com a função predefinida `backup` para acessar o SVM de administrador`engCluster` usando uma senha. Você será solicitado a digitar a senha depois de digitar o comando.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

Ativar contas de chave pública SSH

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou SVM de dados com uma chave pública SSH.

Sobre esta tarefa

- Você deve associar a chave pública à conta antes que a conta possa acessar o SVM.

  Associar uma chave pública a uma conta de utilizador

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

Se quiser ativar o modo FIPS no cluster, as contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado. As contas devem ser reconfiguradas antes de ativar o FIPS ou a autenticação do administrador falhar.

A tabela a seguir indica algoritmos de tipo de chave de host compatíveis com conexões SSH ONTAP. Esses tipos de chave não se aplicam à configuração da autenticação pública SSH.

Lançamento do ONTAP	Tipos de chave compatíveis no modo FIPS	Tipos de chave compatíveis no modo não FIPS
9.11.1 e mais tarde	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 e rsa-sha2-512 e rsa-sha2-256 e ssh-ed25519 e ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss e ssh-rsa

O suporte para o algoritmo de chave de host ssh-ed25519 é removido a partir de ONTAP 9.11,1.

Para obter mais informações, "Configurar a segurança da rede usando o FIPS"consulte .

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Habilite as contas de administrador local para acessar um SVM usando uma chave pública SSH:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir permite que a conta de administrador SVM `svmadmin1` com a função predefinida `vsadmin-volume` acesse o SVM`engData1` usando uma chave pública SSH:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

Depois de terminar

Se você não tiver associado uma chave pública à conta de administrador, deverá fazê-lo antes que a conta possa acessar o SVM.

Associar uma chave pública a uma conta de utilizador

Habilitar contas de autenticação multifator (MFA)

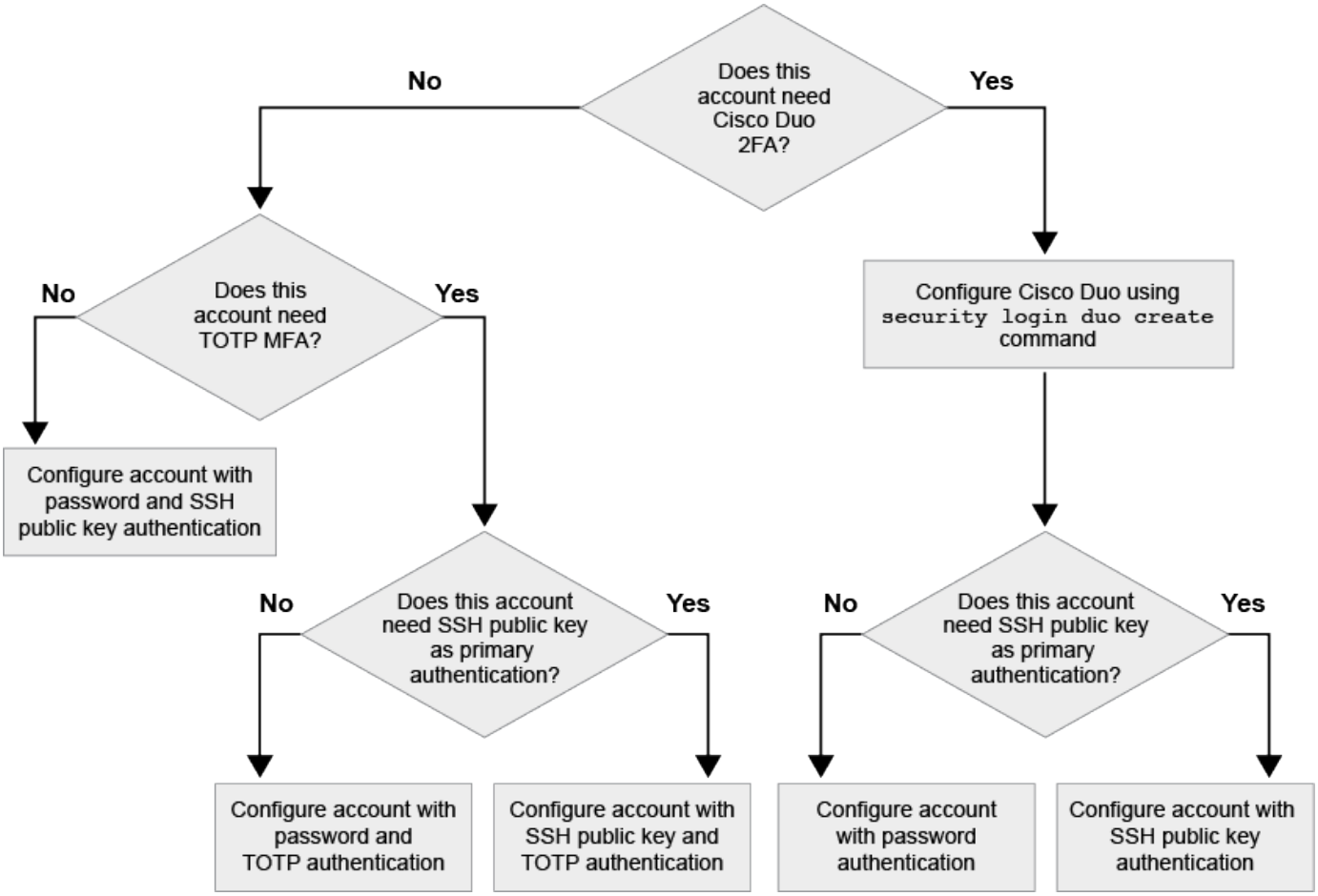
Visão geral da autenticação multifator

A autenticação multifator (MFA) permite aprimorar a segurança, exigindo que os usuários forneçam dois métodos de autenticação para fazer login em um administrador ou uma VM de storage de dados.

Dependendo da sua versão do ONTAP, você pode usar uma combinação de uma chave pública SSH, uma senha de usuário e uma senha única baseada em tempo (TOTP) para autenticação multifator. Quando você ativa e configura o Cisco Duo (ONTAP 9.14,1 e posterior), ele serve como um método de autenticação adicional, complementando os métodos existentes para todos os usuários.

Disponível a partir de…	Primeiro método de autenticação	Segundo método de autenticação
ONTAP 9.14,1	Chave pública SSH	TOTP
	Palavra-passe do utilizador	TOTP
	Chave pública SSH	Cisco Duo
	Palavra-passe do utilizador	Cisco Duo
ONTAP 9.13,1	Chave pública SSH	TOTP
	Palavra-passe do utilizador	TOTP
ONTAP 9,3	Chave pública SSH	Palavra-passe do utilizador

Se o MFA estiver configurado, o administrador do cluster deve primeiro habilitar a conta de usuário local e, em seguida, a conta deve ser configurada pelo usuário local.



Ativar a autenticação multifator

Com a autenticação multifator (MFA), você aumenta a segurança, exigindo que os

usuários forneçam dois métodos de autenticação para fazer login em um administrador ou SVM de dados.

Sobre esta tarefa

- Você deve ser um administrador de cluster para executar esta tarefa.
- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

  "Modificação da função atribuída a um administrador"

- Se você estiver usando uma chave pública para autenticação, associe a chave pública à conta antes que a conta possa acessar o SVM.

  "Associar uma chave pública a uma conta de utilizador"

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- A partir do ONTAP 9.12,1, você pode usar dispositivos de autenticação de hardware Yubikey para o MFA do cliente SSH usando os padrões de autenticação FIDO2 (identidade rápida on-line) ou Verificação de identidade pessoal (PIV).

Habilite o MFA com chave pública SSH e senha do usuário

A partir do ONTAP 9.3, um administrador de cluster pode configurar contas de usuário locais para fazer login com MFA usando uma chave pública SSH e uma senha de usuário.

1. Habilite o MFA em conta de usuário local com chave pública SSH e senha de usuário:

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   O comando a seguir exige que a conta de administrador SVM `admin2` com a função predefinida `admin` efetue login no SVM`engData1` com uma chave pública SSH e uma senha de usuário:

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

Habilite MFA com TOTP

A partir do ONTAP 9.13,1, você pode melhorar a segurança, exigindo que os usuários locais façam login em um administrador ou SVM de dados com uma chave pública SSH ou senha de usuário e uma senha única

baseada em tempo (TOTP). Depois que a conta estiver habilitada para MFA com TOTP, o usuário local deverá fazer login "conclua a configuração"no .

TOTP é um algoritmo de computador que usa a hora atual para gerar uma senha única. Se o TOTP for usado, é sempre a segunda forma de autenticação após a chave pública SSH ou a senha do usuário.

Antes de começar

Você deve ser um administrador de armazenamento para executar essas tarefas.

Passos

Você pode configurar o MFA para com uma senha de usuário ou uma chave pública SSH como o primeiro método de autenticação e o TOTP como o segundo método de autenticação.

Habilite MFA com senha de usuário e TOTP

1. Ative uma conta de usuário para autenticação multifator com uma senha de usuário e TOTP.

   Para novas contas de usuário

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Para contas de usuário existentes

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Verifique se o MFA com TOTP está ativado:

   ```
   security login show
   ```

Habilite MFA com chave pública SSH e TOTP

1. Ative uma conta de usuário para autenticação multifator com uma chave pública SSH e TOTP.

   Para novas contas de usuário

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Para contas de usuário existentes

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Verifique se o MFA com TOTP está ativado:

```
security login show
```

Depois de terminar

- Se você não tiver associado uma chave pública à conta de administrador, deverá fazê-lo antes que a conta possa acessar o SVM.

  "Associar uma chave pública a uma conta de utilizador"

- O usuário local deve fazer login para concluir a configuração de MFA com TOTP.

  "Configurar conta de usuário local para MFA com TOTP"

Informações relacionadas

Saiba mais "Autenticação multifator no ONTAP 9 (TR-4647)"sobre o .

Configurar conta de usuário local para MFA com TOTP

A partir do ONTAP 9.13,1, as contas de usuário podem ser configuradas com autenticação multifator (MFA) usando uma senha única baseada em tempo (TOTP).

Antes de começar

- O administrador de armazenamento tem de "Habilite MFA com TOTP" ser um segundo método de autenticação para a sua conta de utilizador.
- Seu método de autenticação de conta de usuário principal deve ser uma senha de usuário ou uma chave SSH pública.
- Você deve configurar seu aplicativo TOTP para trabalhar com seu smartphone e criar sua chave secreta TOTP.

  Microsoft Authenticator, Google Authenticator, Authy e qualquer outro autenticador compatível com TOTP são suportados.

Passos

1. Inicie sessão na sua conta de utilizador com o método de autenticação atual.

   Seu método de autenticação atual deve ser uma senha de usuário ou uma chave pública SSH.

2. Crie a configuração TOTP na sua conta:

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Verifique se a configuração TOTP está ativada na sua conta:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

Repor chave secreta TOTP

Para proteger a segurança da sua conta, se a sua chave secreta TOTP estiver comprometida ou perdida, você deve desativá-la e criar uma nova.

Reponha o TOTP se a sua chave estiver comprometida

Se sua chave secreta TOTP estiver comprometida, mas você ainda tiver acesso a ela, poderá remover a chave comprometida e criar uma nova.

1. Faça login na sua conta de usuário com sua senha de usuário ou chave pública SSH e sua chave secreta TOTP comprometida.
2. Remova a chave secreta TOTP comprometida:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Crie uma nova chave secreta TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Verifique se a configuração TOTP está ativada na sua conta:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Reinicie o TOTP se a sua chave for perdida

Se a chave secreta TOTP for perdida, entre em Contato com o administrador de armazenamento para "tenha a chave desativada". Depois que sua chave for desativada, você poderá usar seu primeiro método de autenticação para fazer login e configurar um novo TOTP.

Antes de começar

A chave secreta TOTP deve ser desativada por um administrador de armazenamento. Se não tiver uma conta de administrador de armazenamento, contacte o administrador de armazenamento para desativar a chave.

Passos

1. Depois que o segredo TOTP for desativado por um administrador de armazenamento, use seu método de autenticação principal para fazer login na sua conta local.

2. Crie uma nova chave secreta TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Verifique se a configuração TOTP está ativada na sua conta:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Desative a chave secreta TOTP para a conta local

Se a chave secreta de uma senha de tempo único (TOTP) de um usuário local for perdida, a chave perdida deve ser desativada por um administrador de armazenamento antes que o usuário possa criar uma nova chave secreta TOTP.

Sobre esta tarefa

Esta tarefa só pode ser executada a partir de uma conta de administrador de cluster.

Passo

1. Desative a chave secreta TOTP:

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

Ativar contas de certificado SSL

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou data SVM com um certificado SSL.

Sobre esta tarefa

- Você deve instalar um certificado digital de servidor assinado pela CA antes que a conta possa acessar o SVM.

  Gerando e instalando um certificado de servidor assinado pela CA

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, poderá adicionar a função mais tarde com o `security login modify` comando.

  Modificação da função atribuída a um administrador

Para contas de administrador de cluster, a autenticação de certificado é suportada com os `http` aplicativos , `ontapi` e `rest` . Para contas de administrador da SVM, a autenticação de certificado é compatível apenas com `ontapi` os aplicativos e `rest` .

Passo

1. Ative as contas de administrador local para acessar um SVM usando um certificado SSL:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Para obter a sintaxe de comando completa, consulte "ONTAP man pages por release".

   O comando a seguir permite que a conta de administrador SVM `svmadmin2` com a função padrão `vsadmin` acesse o SVM`engData2` usando um certificado digital SSL.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

Depois de terminar

Se você não tiver instalado um certificado digital de servidor assinado pela CA, deverá fazê-lo antes que a conta possa acessar o SVM.

Gerando e instalando um certificado de servidor assinado pela CA

Ative o acesso à conta do ative Directory

Você pode usar o `security login create` comando para habilitar contas de usuário ou grupo do ative Directory (AD) para acessar um administrador ou SVM de dados. Qualquer usuário do grupo AD pode acessar o SVM com a função atribuída ao grupo.

Sobre esta tarefa

- Você deve configurar o acesso do controlador de domínio do AD ao cluster ou SVM antes que a conta possa acessar o SVM.

  Configurando o acesso do controlador de domínio do ative Directory

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- A partir do ONTAP 9.13,1, você pode usar uma chave pública SSH como seu método de autenticação principal ou secundário com uma senha de usuário do AD.

  Se você optar por usar uma chave pública SSH como sua autenticação principal, nenhuma autenticação AD ocorrerá.

- A partir do ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch" se for suportado pelo servidor LDAP do AD.
- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

Modificação da função atribuída a um administrador

O acesso à conta do GRUPO DE ANÚNCIOS é suportado apenas com os `SSH` aplicativos , `ontapi` e `rest` . Grupos DE ANÚNCIOS não são suportados com autenticação de chave pública SSH, que é comumente usada para autenticação multifator.

Antes de começar

- O tempo do cluster deve ser sincronizado dentro de cinco minutos do tempo no controlador de domínio do AD.
- Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Habilite contas de administrador de grupo ou usuário do AD para acessar um SVM:

   Para usuários do AD:

Versão de ONTAP	Autenticação primária	Autenticação secundária	Comando
9.13.1 e mais tarde	Chave pública	Nenhum	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

9.13.1 e mais tarde	Domínio	Chave pública	**Para um novo usuário**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Para um usuário existente
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

Versão de ONTAP	Autenticação primária	Autenticação secundária	Comando
9,0 e mais tarde	Domínio	Nenhum	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Para grupos AD:

Versão de ONTAP	Autenticação primária	Autenticação secundária	Comando
9,0 e mais tarde	Domínio	Nenhum	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Para obter a sintaxe de comando completa, consulte "Planilhas para autenticação de administrador e configuração RBAC"

Depois de terminar

Se você não tiver configurado o acesso do controlador de domínio do AD ao cluster ou SVM, deverá fazê-lo antes que a conta possa acessar o SVM.

Configurando o acesso do controlador de domínio do ative Directory

Ative o acesso a contas LDAP ou NIS

Você pode usar o `security login create` comando para habilitar contas de usuário LDAP ou NIS para acessar um administrador ou SVM de dados. Se você não tiver configurado o acesso de servidor LDAP ou NIS ao SVM, deverá fazê-lo antes que a conta possa acessar o SVM.

Sobre esta tarefa

- As contas de grupo não são suportadas.
- Você deve configurar o acesso de servidor LDAP ou NIS ao SVM antes que a conta possa acessar o SVM.

Configurando o acesso ao servidor LDAP ou NIS

Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

  Modificação da função atribuída a um administrador

- A partir do ONTAP 9.4, a autenticação multifator (MFA) é compatível com usuários remotos em servidores LDAP ou NIS.
- A partir do ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch" se for suportado pelo servidor LDAP.
- Devido a um problema LDAP conhecido, você não deve usar o `':'` caractere (dois pontos) em nenhum campo de informações de conta de usuário LDAP (por exemplo, `gecos` `userPassword` , e assim por diante). Caso contrário, a operação de pesquisa falhará para esse usuário.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Habilite contas de usuário ou grupo LDAP ou NIS para acessar um SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   "Criando ou modificando contas de login"

   O comando a seguir habilita a conta de administrador de cluster LDAP ou NIS `guest2` com a função predefinida `backup` para acessar o SVM admin`engCluster` .

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. Ativar login MFA para usuários LDAP ou NIS:

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh
   -authentication-method nsswitch -role admin -is-ns-switch-group no -second
   -authentication-method publickey
   ```

   O método de autenticação pode ser especificado como `publickey` e segundo método de autenticação `nsswitch` como .

   O exemplo a seguir mostra a autenticação MFA sendo ativada:

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2
   -application ssh -authentication-method nsswitch -vserver
   cluster-1 -second-authentication-method publickey"
   ```

Depois de terminar

Se você não tiver configurado o acesso de servidor LDAP ou NIS ao SVM, deverá fazê-lo antes que a conta possa acessar o SVM.

Configurando o acesso ao servidor LDAP ou NIS

Gerenciar funções de controle de acesso

Gerencie a visão geral das funções de controle de acesso

A função atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Modifique a função atribuída a um administrador

Você pode usar o `security login modify` comando para alterar a função de uma conta de administrador de cluster ou SVM. Pode atribuir uma função predefinida ou personalizada.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Alterar a função de um administrador de cluster ou SVM:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   "Criando ou modificando contas de login"

   O comando a seguir altera a função da conta de administrador do cluster do AD `DOMAIN1\guest1` para a função predefinida `readonly`.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   O comando a seguir altera a função das contas de administrador do SVM na conta do grupo AD `DOMAIN1\adgroup` para a função personalizada `vol_role`.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

Definir funções personalizadas

Você pode usar o `security login role create` comando para definir uma função personalizada. Você pode executar o comando quantas vezes for necessário para obter a combinação exata de recursos que deseja associar à função.

Sobre esta tarefa

- Uma função, predefinida ou personalizada, concede ou nega acesso a comandos ou diretórios de comandos do ONTAP.

  Um diretório de comandos (`volume`, por exemplo) é um grupo de comandos e subdiretórios de comandos relacionados. Exceto conforme descrito neste procedimento, conceder ou negar acesso a um diretório de comando concede ou nega acesso a cada comando no diretório e seus subdiretórios.

- O acesso a comandos específicos ou o acesso a subdiretórios substitui o acesso ao diretório pai.

  Se uma função for definida com um diretório de comando e, em seguida, for definida novamente com um nível de acesso diferente para um comando específico ou para um subdiretório do diretório pai, o nível de acesso especificado para o comando ou subdiretório substitui o do pai.

> Não é possível atribuir a um administrador SVM uma função que dê acesso a um diretório de comando ou comando que esteja disponível apenas para o `admin` administrador de cluster - por exemplo, o `security` diretório de comando.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Definir uma função personalizada:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   Os comandos a seguir concedem à `vol_role` função acesso total aos comandos no `volume` diretório de comandos e acesso somente leitura aos comandos `volume snapshot` no subdiretório.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   Os comandos a seguir concedem à `SVM_storage` função acesso somente leitura aos comandos no `storage` diretório de comandos, sem acesso aos comandos `storage encryption` no subdiretório e acesso total ao `storage aggregate plex offline` comando não intrínseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Funções predefinidas para administradores de cluster

As funções predefinidas para administradores de cluster devem atender à maioria das suas necessidades. Você pode criar funções personalizadas conforme necessário. Por padrão, um administrador de cluster recebe a função predefinida `admin`.

A tabela a seguir lista as funções predefinidas para administradores de cluster:

Esta função…	Tem este nível de acesso…	Para os seguintes comandos ou diretórios de comandos
administrador	tudo	Todos os diretórios de comando (`DEFAULT`)
admin-no-fsa (disponível a partir de ONTAP 9.12,1)	Leitura/escrita	• Todos os diretórios de comando (`DEFAULT`) • `security login rest-role` • `security login role`

Somente leitura	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Nenhum
`volume file show-disk-usage`	AutoSupport	tudo
• `set` • `system node autosupport`	nenhum	Todos os outros diretórios de comando (`DEFAULT`)
backup	tudo	`vserver services ndmp`
readonly	`volume`	nenhum
Todos os outros diretórios de comando (`DEFAULT`)	readonly	tudo

• `security login password` Apenas para gerir a palavra-passe local da conta de utilizador e as informações das chaves • `set`	nenhum	`security`
readonly	Todos os outros diretórios de comando (`DEFAULT`)	SnapLock
tudo	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	nenhum
• `volume move governor` • `volume move recommend`	nenhum	Todos os outros diretórios de comando (`DEFAULT`)
nenhum	nenhum	Todos os diretórios de comando (`DEFAULT`)

A `autosupport` função é atribuída à conta predefinida `autosupport`, que é usada pelo AutoSupport OnDemand. O ONTAP impede que você modifique ou exclua a `autosupport` conta. O ONTAP também impede que você atribua `autosupport` a função a outras contas de usuário.

Funções predefinidas para administradores de SVM

As funções predefinidas para administradores de SVM devem atender à maioria das suas necessidades. Você pode criar funções personalizadas conforme necessário. Por padrão, a função predefinida é atribuída a um administrador SVM `vsadmin`.

A tabela a seguir lista as funções predefinidas para administradores de SVM:

Nome da função	Recursos

vsadmin	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, exceto movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Gerenciamento de LUNs • Executando operações SnapLock, exceto exclusão privilegiada • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Tarefas de monitorização • Monitoramento de conexões de rede e interface de rede • Monitoramento da integridade do SVM
vsadmin-volume	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, incluindo movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Gerenciamento de LUNs • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Monitorização da interface de rede • Monitoramento da integridade do SVM
protocolo vsadmin	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Gerenciamento de LUNs • Monitorização da interface de rede • Monitoramento da integridade do SVM

vsadmin-backup	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de operações NDMP • Fazendo uma leitura/gravação de volume restaurada • Gerenciamento de relacionamentos do SnapMirror e cópias Snapshot • Visualização de volumes e informações de rede
vsadmin-SnapLock	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, exceto movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Executar operações SnapLock, incluindo exclusão privilegiada • Configurando protocolos: NFS e SMB • Configurando serviços: DNS, LDAP e NIS • Tarefas de monitorização • Monitoramento de conexões de rede e interface de rede
vsadmin-readonly	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Monitoramento da integridade do SVM • Monitorização da interface de rede • Visualização de volumes e LUNs • Visualização de serviços e protocolos

Controle o acesso do administrador

A função atribuída a um administrador determina quais funções o administrador pode executar com o System Manager. Funções predefinidas para administradores de cluster e administradores de VM de storage são fornecidas pelo System Manager. Você atribui a função ao criar a conta do administrador ou pode atribuir uma função diferente posteriormente.

Dependendo de como você ativou o acesso à conta, talvez seja necessário executar qualquer um dos seguintes procedimentos:

- Associar uma chave pública a uma conta local.
- Instale um certificado digital de servidor assinado pela CA.

- Configure o acesso AD, LDAP ou NIS.

Você pode executar essas tarefas antes ou depois de ativar o acesso à conta.

Atribuindo uma função a um administrador

Atribua uma função a um administrador, da seguinte forma:

Passos

1. Selecione **Cluster > Settings**.
2. Selecione → ao lado de **usuários e funções**.
3. + Add Selecione em **Users**.
4. Especifique um nome de usuário e selecione uma função no menu suspenso **role**.
5. Especifique um método de login e uma senha para o usuário.

Alterar a função de administrador

Altere a função de um administrador, da seguinte forma:

Passos

1. Clique em **Cluster > Settings**.
2. Selecione o nome do usuário cuja função deseja alterar e clique no ⋮ que aparece ao lado do nome de usuário.
3. Clique em **Editar**.
4. Selecione uma função no menu suspenso **Role**.

Gerenciar contas de administrador

Visão geral das contas de administrador

Dependendo de como você ativou o acesso à conta, talvez seja necessário associar uma chave pública a uma conta local, instalar um certificado digital de servidor assinado pela CA ou configurar o acesso AD, LDAP ou NIS. Você pode executar todas essas tarefas antes ou depois de ativar o acesso à conta.

Associar uma chave pública a uma conta de administrador

Para autenticação de chave pública SSH, você deve associar a chave pública a uma conta de administrador antes que a conta possa acessar o SVM. Você pode usar o `security login publickey create` comando para associar uma chave a uma conta de administrador.

Sobre esta tarefa

Se você autenticar uma conta via SSH com uma senha e uma chave pública SSH, a conta será autenticada primeiro com a chave pública.

Antes de começar

- Você deve ter gerado a chave SSH.

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Associar uma chave pública a uma conta de administrador:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   Para obter a sintaxe de comando completa, consulte a referência de Planilha para "Associar uma chave pública a uma conta de utilizador".

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir associa uma chave pública à conta de administrador do SVM `svmadmin1` para o `engData1` SVM . A chave pública recebe o número de índice 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Gerenciar chaves públicas SSH e certificados X,509 para uma conta de administrador

Para maior segurança de autenticação SSH com contas de administrador, você pode usar o `security login publickey` conjunto de comandos para gerenciar a chave pública SSH e sua associação com certificados X,509.

Associar uma chave pública e um certificado X,509 a uma conta de administrador

A partir do ONTAP 9.13,1, é possível associar um certificado X,509 à chave pública associada à conta de administrador. Isso dá a você a segurança adicional de verificações de expiração ou revogação de certificados no login SSH para essa conta.

Sobre esta tarefa

Se você autenticar uma conta via SSH com uma chave pública SSH e um certificado X,509, o ONTAP verifica a validade do certificado X,509 antes de autenticar com a chave pública SSH. O login SSH será recusado se esse certificado estiver expirado ou revogado, e a chave pública será automaticamente desativada.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Você deve ter gerado a chave SSH.
- Se você precisar apenas do certificado X,509 para ser verificado para a expiração, você pode usar um certificado autoassinado.
- Se você precisar que o certificado X,509 seja verificado quanto à expiração e revogação:
  - Você deve ter recebido o certificado de uma autoridade de certificação (CA).

- Você deve instalar a cadeia de certificados (certificados de CA intermediária e raiz) usando `security certificate install` comandos.
- Você precisa ativar o OCSP para SSH. "Verifique se os certificados digitais são válidos usando OCSP"Consulte para obter instruções.

Passos

1. Associar uma chave pública e um certificado X,509 a uma conta de administrador:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   Para obter a sintaxe de comando completa, consulte a referência de Planilha para "Associar uma chave pública a uma conta de utilizador".

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir associa uma chave pública e um certificado X,509 à conta de administrador do SVM `svmadmin2` para o `engData2` SVM . A chave pública recebe o número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Remova a associação de certificados da chave pública SSH para uma conta de administrador

Você pode remover a associação de certificados atual da chave pública SSH da conta, mantendo a chave pública.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Remova a associação de certificados X,509 de uma conta de administrador e guarde a chave pública SSH existente:

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir remove a associação de certificado X,509 da conta de administrador SVM `svmadmin2` para SVM `engData2` no índice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Remova a associação de chave pública e certificado de uma conta de administrador

Você pode remover a chave pública atual e a configuração de certificado de uma conta.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Remova a chave pública e uma associação de certificado X,509 de uma conta de administrador:

   `security login publickey delete -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir remove uma chave pública e um certificado X,509 da conta de administrador do SVM `svmadmin3` para o SVM `engData3` no índice 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Configure o Cisco Duo 2FA para logins SSH com o ONTAP

A partir do ONTAP 9.14,1, você pode configurar o ONTAP para usar o Cisco Duo para autenticação de dois fatores (2FA) durante logins SSH. Você configura o Duo no nível do cluster e se aplica a todas as contas de usuário por padrão. Como alternativa, você pode configurar o Duo no nível da VM de armazenamento (anteriormente chamado de vserver), caso em que ele se aplica apenas aos usuários dessa VM de armazenamento. Se você ativar e configurar o Duo, ele serve como um método de autenticação adicional, complementando os métodos existentes para todos os usuários.

Se você ativar a autenticação Duo para logins SSH, os usuários precisarão Registrar um dispositivo na próxima vez que fizerem login usando SSH. Para obter informações sobre a inscrição, consulte o Cisco "documentação de inscrição" Duo .

Você pode usar a interface de linha de comando ONTAP para executar as seguintes tarefas com o Cisco Duo:

- Configure o Cisco Duo
- Altere a configuração do Cisco Duo
- Remova a configuração do Cisco Duo
- Veja a configuração do Cisco Duo
- Remova um grupo Duo
- Ver grupos Duo
- Ignorar a autenticação Duo para usuários

Configure o Cisco Duo

Você pode criar uma configuração do Cisco Duo para todo o cluster ou para uma VM de armazenamento específica (chamada de vserver na CLI do ONTAP) usando o[`security login duo create` comando. Quando você faz isso, o Cisco Duo é habilitado para logins SSH para esse cluster ou VM de armazenamento. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-create.html[`security login duo create`em referência de comando ONTAP.

Passos

1. Inicie sessão no Painel de Administração do Cisco Duo.
2. Aceda a **aplicações > aplicação UNIX**.
3. Registre sua chave de integração, chave secreta e nome de host da API.
4. Faça login na sua conta ONTAP usando SSH.
5. Ative a autenticação do Cisco Duo para esta VM de armazenamento, substituindo as informações do seu ambiente pelos valores entre parênteses:

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Saiba mais sobre o comando no "Planilhas para autenticação de administrador e configuração RBAC".

Altere a configuração do Cisco Duo

Você pode alterar a maneira como o Cisco Duo autentica os usuários (por exemplo, quantos prompts de autenticação são fornecidos ou qual proxy HTTP é usado). Se você precisar alterar a configuração do Cisco Duo para uma VM de armazenamento (chamada de vserver na CLI do ONTAP), use o[`security login duo modify` comando. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-modify.html[`security login duo modify`em referência de comando ONTAP.

Passos

1. Inicie sessão no Painel de Administração do Cisco Duo.
2. Aceda a **aplicações > aplicação UNIX**.
3. Registre sua chave de integração, chave secreta e nome de host da API.
4. Faça login na sua conta ONTAP usando SSH.

5. Altere a configuração do Cisco Duo para esta VM de armazenamento, substituindo as informações atualizadas do seu ambiente pelos valores entre parênteses:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

Remova a configuração do Cisco Duo

Você pode remover a configuração do Cisco Duo, que removerá a necessidade de os usuários SSH se autenticarem usando o Duo no início de sessão. Para remover a configuração do Cisco Duo para uma VM de armazenamento (conhecida como vserver na CLI do ONTAP), você pode usar o[`security login duo delete` comando. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-delete.html[`security login duo delete`em referência de comando ONTAP.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Remova a configuração do Cisco Duo para esta VM de armazenamento, substituindo o nome da VM de armazenamento por `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

Isso exclui permanentemente a configuração do Cisco Duo para essa VM de armazenamento.

Veja a configuração do Cisco Duo

Você pode exibir a configuração existente do Cisco Duo para uma VM de armazenamento (chamada de vserver na CLI do ONTAP) usando o[`security login duo show` comando. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-show.html[`security login duo show`em referência de comando ONTAP.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Mostrar a configuração do Cisco Duo para esta VM de armazenamento. Opcionalmente, você pode usar o `vserver` parâmetro para especificar uma VM de armazenamento, substituindo o nome da VM de armazenamento por `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Você deve ver saída semelhante ao seguinte:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Crie um grupo Duo

Você pode instruir o Cisco Duo a incluir somente os usuários em um determinado ative Directory, LDAP ou grupo de usuários local no processo de autenticação Duo. Se você criar um grupo Duo, somente os usuários desse grupo serão solicitados a autenticação Duo. Você pode criar um grupo Duo usando o[`security login duo group create` comando. Quando você cria um grupo, você pode excluir usuários específicos desse grupo do processo de autenticação Duo. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-group-create.html[`security login duo group create`em referência de comando ONTAP.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Crie o grupo Duo, substituindo as informações do seu ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será criado no nível do cluster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local. Os usuários que você especificar com o parâmetro opcional `-exclude-users` não serão incluídos no processo de autenticação Duo.

Ver grupos Duo

Você pode exibir entradas de grupo existentes do Cisco Duo usando o[`security login duo group show` comando. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-

group-show.html[`security login duo group show`em referência de comando ONTAP.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Mostre as entradas do grupo Duo, substituindo as informações do seu ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será mostrado no nível do cluster:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local. Os usuários que você especificar com o parâmetro opcional `-exclude-users` não serão exibidos.

Remova um grupo Duo

Você pode remover uma entrada de grupo Duo usando o[`security login duo group delete` comando. Se você remover um grupo, os usuários desse grupo não serão mais incluídos no processo de autenticação Duo. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli//security-login-duo-group-delete.html[`security login duo group delete`em referência de comando ONTAP.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Remova a entrada do grupo Duo, substituindo as informações do ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será removido no nível do cluster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local.

Ignorar a autenticação Duo para usuários

Você pode excluir todos os usuários ou usuários específicos do processo de autenticação Duo SSH.

Excluir todos os usuários Duo

Você pode desativar a autenticação SSH do Cisco Duo para todos os usuários.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Desative a autenticação Cisco Duo para usuários SSH, substituindo o nome do SVM para `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

Excluir usuários do grupo Duo

Você pode excluir certos usuários que fazem parte de um grupo Duo do processo de autenticação Duo SSH.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Desative a autenticação Cisco Duo para usuários específicos em um grupo. Substitua o nome do grupo e a lista de usuários para excluir pelos valores entre parênteses:

```
security login group modify -group-name <GROUP_NAME> -exclude-users
<USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local. Os usuários que você especificar com o `-exclude-users` parâmetro não serão incluídos no processo de autenticação Duo.

Excluir usuários locais Duo

Você pode excluir usuários locais específicos do uso da autenticação Duo usando o Painel de Administração do Cisco Duo. Para obter instruções, consulte "Documentação do Cisco Duo" a .

Gere e instale uma visão geral do certificado de servidor assinado pela CA

Em sistemas de produção, é uma prática recomendada instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou SVM como um servidor SSL. Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR) e o `security certificate install` comando para instalar o certificado recebido de volta da autoridade de certificação.

Gerar uma solicitação de assinatura de certificado

Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR). Depois de processar sua solicitação, a autoridade de certificação (CA) envia o certificado digital assinado.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Gerar um CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

O comando a seguir cria uma CSR com uma chave privada de 2048 bits gerada pela função de hash "'SHA256'" para uso pelo grupo "'Software'" no departamento de TI de uma empresa cujo nome comum personalizado é "erver1.companyname.com`", localizado em Sunnyvale, Califórnia, EUA. O endereço de e-mail do administrador de Contato da SVM é "'web@example.com". O sistema apresenta a CSR e a

chave privada na saída.

Exemplo de criação de uma CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. Copie a solicitação de certificado da saída CSR e envie-a em formato eletrônico (como e-mail) para uma CA de terceiros confiável para assinatura.

   Após processar sua solicitação, a CA envia o certificado digital assinado. Você deve manter uma cópia da chave privada e do certificado digital assinado pela CA.

Instale um certificado de servidor assinado pela CA

Você pode usar o `security certificate install` comando para instalar um certificado de servidor assinado pela CA em um SVM. O ONTAP solicita os certificados raiz e intermediário da autoridade de certificação (CA) que formam a cadeia de certificados do certificado do servidor.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Instale um certificado de servidor assinado pela CA:

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   > O ONTAP solicita os certificados raiz e intermediários da CA que formam a cadeia de certificados do certificado do servidor. A cadeia começa com o certificado da CA que emitiu o certificado do servidor e pode variar até o certificado raiz da CA. Qualquer certificado intermediário ausente resulta na falha da instalação do certificado do servidor.

   O comando a seguir instala o certificado de servidor assinado pela CA e os certificados intermediários na SVM "'engData2".

Exemplo de instalação de certificados intermediários de certificado de servidor assinado pela CA

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Gerencie certificados com o System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para gerenciar autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais (integradas).

Com o System Manager, você pode gerenciar os certificados recebidos de outros aplicativos para que você possa autenticar as comunicações desses aplicativos. Você também pode gerenciar seus próprios certificados que identificam seu sistema para outros aplicativos.

Exibir informações do certificado

Com o System Manager, é possível exibir autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais armazenadas no cluster.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Role até a área **Segurança**. Na seção **certificados**, os seguintes detalhes são exibidos:
   - O número de autoridades de certificação confiáveis armazenadas.
   - O número de certificados de cliente/servidor armazenados.
   - O número de autoridades locais de certificação armazenadas.
3. Selecione qualquer número para ver detalhes sobre uma categoria de certificados ou →selecione para abrir a página **certificados**, que contém informações sobre todas as categorias. A lista exibe as informações de todo o cluster. Se você quiser exibir informações apenas para uma VM de armazenamento específica, execute as seguintes etapas:
   a. Selecione **Storage > Storage VMs**.
   b. Selecione a VM de armazenamento.
   c. Mude para o separador **Settings**.

d. Selecione um número mostrado na seção **certificado**.

O que fazer a seguir

- Na página **certificados**, você pode Gerar uma solicitação de assinatura de certificado.
- As informações do certificado são separadas em três guias, uma para cada categoria. Você pode executar as seguintes tarefas em cada guia:

Neste separador…	Pode executar estes procedimentos…
Autoridades de certificação confiáveis	• [install-trusted-cert] • Excluir uma autoridade de certificação confiável • Renove uma autoridade de certificação confiável
Certificados de cliente/servidor	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• Autoridades de certificação locais*	• Crie uma nova autoridade de certificação local • Assine um certificado usando uma autoridade de certificação local • Eliminar uma autoridade de certificação local • Renove uma autoridade de certificação local

Gerar uma solicitação de assinatura de certificado

Você pode gerar uma solicitação de assinatura de certificado (CSR) com o System Manager a partir de qualquer guia da página **certificados**. Uma chave privada e uma CSR correspondente são geradas, que podem ser assinadas usando uma autoridade de certificação para gerar um certificado público.

Passos

1. Veja a página **certificados**. Exibir informações do certificadoConsulte .
2. Selecione * gerar CSR*.
3. Preencha as informações para o nome do assunto:
   a. Introduza um **nome comum**.
   b. Selecione um **país**.
   c. Introduza uma **organização**.
   d. Introduza uma **unidade organizacional**.
4. Se você quiser substituir os padrões, selecione **mais opções** e forneça informações adicionais.

Instale (adicione) uma autoridade de certificação confiável

Você pode instalar autoridades de certificação confiáveis adicionais no System Manager.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. Exibir informações do certificadoConsulte .

2. + Add Selecione .
3. No painel **Adicionar autoridade de certificação confiável**, execute o seguinte:
   - Introduza um **nome**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
   - Selecione um **tipo**.
   - Introduza ou importe **detalhes do certificado**.

Excluir uma autoridade de certificação confiável

Com o System Manager, você pode excluir uma autoridade de certificação confiável.

Não é possível excluir autoridades de certificado confiáveis pré-instaladas com o ONTAP.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação fidedigna.
3. Selecione ⋮ ao lado do nome e selecione **Excluir**.

Renove uma autoridade de certificação confiável

Com o System Manager, você pode renovar uma autoridade de certificação confiável que expirou ou está prestes a expirar.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação fidedigna.
3. Selecione ⋮ ao lado do nome do certificado e depois **Renew**.

Instale (adicione) um certificado cliente/servidor

Com o System Manager, você pode instalar certificados de cliente/servidor adicionais.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. + Add Selecione .
3. No painel **Adicionar certificado de cliente/servidor**, execute o seguinte:
   - Introduza um **nome de certificado**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
   - Selecione um **tipo**.
   - Introduza ou importe **detalhes do certificado**. Você pode escrever ou copiar e colar os detalhes do certificado de um arquivo de texto ou importar o texto de um arquivo de certificado clicando em **Importar**.

- Introduza a **chave privada**. Você pode escrever ou copiar e colar na chave privada de um arquivo de texto ou pode importar o texto de um arquivo de chave privada clicando em **Importar**.

Gerar (adicionar) um certificado cliente/servidor autoassinado

Com o System Manager, você pode gerar certificados de cliente/servidor autoassinados adicionais.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. Selecione * gerar certificado autoassinado*.
3. No painel **Generate Self-signed Certificate** (gerar certificado autoassinado), execute o seguinte procedimento:
   - Introduza um **nome de certificado**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
   - Selecione um **tipo**.
   - Selecione uma função **hash**.
   - Selecione um **tamanho da chave**.
   - Selecione uma **VM de armazenamento**.

Excluir um certificado cliente/servidor

Com o System Manager, pode eliminar certificados de cliente/servidor.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. Selecione o nome do certificado cliente/servidor.
3. Selecione ⋮ ao lado do nome e clique em **Excluir**.

Renove um certificado cliente/servidor

Com o System Manager, você pode renovar um certificado cliente/servidor que expirou ou está prestes a expirar.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. Selecione o nome do certificado cliente/servidor.
3. Selecione ⋮ ao lado do nome e, em seguida, clique em **Renew**.

Crie uma nova autoridade de certificação local

Com o System Manager, você pode criar uma nova autoridade de certificação local.

Passos

1. Veja a guia **autoridades de certificados locais**. Exibir informações do certificadoConsulte .
2. + Add Selecione .

3. No painel **Add local Certificate Authority** (Adicionar autoridade de certificação local), execute o seguinte procedimento:
   - Introduza um **nome**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
4. Se você quiser substituir os padrões, selecione **mais opções** e forneça informações adicionais.

Assine um certificado usando uma autoridade de certificação local

No System Manager, você pode usar uma autoridade de certificação local para assinar um certificado.

Passos

1. Veja a guia **autoridades de certificados locais**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione ⋮ ao lado do nome e depois **assinar um certificado**.
4. Preencha o formulário **assinar um pedido de assinatura de certificado**.
   - Você pode colar no conteúdo de assinatura de certificado ou importar um arquivo de solicitação de assinatura de certificado clicando em **Importar**.
   - Especifique o número de dias para os quais o certificado será válido.

Eliminar uma autoridade de certificação local

Com o System Manager, pode eliminar uma autoridade de certificação local.

Passos

1. Veja a guia **Autoridade de Certificação local**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione ⋮ ao lado do nome e, em seguida, **Excluir**.

Renove uma autoridade de certificação local

Com o System Manager, você pode renovar uma autoridade de certificação local que expirou ou está prestes a expirar.

Passos

1. Veja a guia **Autoridade de Certificação local**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione ⋮ ao lado do nome e, em seguida, clique em **Renew**.

Configure a visão geral do acesso do controlador de domínio do ative Directory

Você deve configurar o acesso do controlador de domínio do AD ao cluster ou SVM antes que uma conta do AD possa acessar o SVM. Se você já tiver configurado um servidor SMB para um SVM de dados, poderá configurar o SVM como um gateway, ou *tunnel*, para acesso AD ao cluster. Se você não tiver configurado um servidor SMB, poderá criar uma conta de computador para o SVM no domínio AD.

O ONTAP oferece suporte aos seguintes serviços de autenticação de controlador de domínio:

- Kerberos
- LDAP
- NETLOGON
- Autoridade de Segurança local (LSA)

O ONTAP suporta os seguintes algoritmos de chave de sessão para conexões seguras de Netlogon:

Algoritmo da chave de sessão	Disponível a partir de…
HMAC-SHA256, com base no padrão de criptografia avançada (AES) se o cluster estiver executando o ONTAP 9.9,1 ou anterior e o controlador de domínio forçar o AES para serviços de Netlogon seguros, a conexão falhará. Nesse caso, você precisa reconfigurar seu controlador de domínio para aceitar conexões de chave forte com o ONTAP.	ONTAP 9.10,1
DES e HMAC-MD5 (quando a chave forte está definida)	Todos os lançamentos do ONTAP 9

Se você quiser usar chaves de sessão AES durante o estabelecimento de canal seguro Netlogon, você precisa verificar se o AES está habilitado no SVM.

- A partir do ONTAP 9.14,1, o AES é ativado por padrão quando você cria um SVM e não precisa modificar as configurações de segurança do seu SVM para usar chaves de sessão AES durante o estabelecimento de canal seguro Netlogon.
- No ONTAP 9.10,1 a 9.13.1, o AES é desativado por padrão quando você cria um SVM. Você precisa ativar o AES usando o seguinte comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

> Quando você atualiza para o ONTAP 9.14,1 ou posterior, a configuração AES para SVMs existentes que foram criadas com versões mais antigas do ONTAP não será alterada automaticamente. Você ainda precisa atualizar o valor dessa configuração para ativar o AES nesses SVMs.

Configurar um túnel de autenticação

Se você já tiver configurado um servidor SMB para um SVM de dados, poderá usar o `security login domain-tunnel create` comando para configurar o SVM como um gateway, ou *tunnel*, para acesso AD ao cluster.

Antes de começar

- Você precisa ter configurado um servidor SMB para um data SVM.
- Você deve ter habilitado uma conta de usuário de domínio do AD para acessar o SVM do administrador do cluster.
- Você deve ser um administrador de cluster para executar esta tarefa.

A partir do ONTAP 9.10,1, se você tiver um gateway SVM (túnel de domínio) para acesso AD, você poderá usar o Kerberos para autenticação de administrador se tiver desabilitado o NTLM no domínio do AD. Em versões anteriores, o Kerberos não era compatível com autenticação de administrador para gateways SVM. Esta funcionalidade está disponível por padrão; nenhuma configuração é necessária.

> A autenticação Kerberos é sempre tentada primeiro. Em caso de falha, a autenticação NTLM é então tentada.

Passo

1. Configure um SVM de dados habilitado para SMB como um túnel de autenticação para acesso do controlador de domínio do AD ao cluster:

   `security login domain-tunnel create -vserver` *`svm_name`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   > O SVM deve estar em execução para que o usuário seja autenticado.

   O comando a seguir configura o SVM de dados habilitado para SMB "'engData" como um túnel de autenticação.

   ```
   cluster1::>security login domain-tunnel create -vserver engData
   ```

Crie uma conta de computador SVM no domínio

Se você não tiver configurado um servidor SMB para um SVM de dados, poderá usar o `vserver active-directory create` comando para criar uma conta de computador para o SVM no domínio.

Sobre esta tarefa

Depois de inserir o `vserver active-directory create` comando, você será solicitado a fornecer as credenciais para uma conta de usuário do AD com Privileges suficiente para adicionar computadores à unidade organizacional especificada no domínio. A senha da conta não pode estar vazia.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Crie uma conta de computador para um SVM no domínio AD:

   `vserver active-directory create -vserver` *`SVM_name`* `-account-name` *`NetBIOS_account_name`* `-domain` *`domain`* `-ou` *`organizational_unit`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir cria uma conta de computador chamada "'ADSERVER1"" no domínio "'example.com`'" para SVM "'engData". Você será solicitado a inserir as credenciais da conta de usuário do AD depois de inserir o comando.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

Configure a visão geral do acesso ao servidor LDAP ou NIS

Você deve configurar o acesso de servidor LDAP ou NIS a um SVM antes que as contas LDAP ou NIS possam acessar o SVM. O recurso de switch permite que você use LDAP ou NIS como fontes alternativas de serviço de nomes.

Configurar o acesso ao servidor LDAP

Você deve configurar o acesso do servidor LDAP a um SVM antes que as contas LDAP possam acessar o SVM. Você pode usar o `vserver services name-service ldap client create` comando para criar uma configuração de cliente LDAP no SVM. Em seguida, você pode usar o `vserver services name-service ldap create` comando para associar a configuração do cliente LDAP ao SVM.

Sobre esta tarefa

A maioria dos servidores LDAP pode usar os esquemas padrão fornecidos pelo ONTAP:

- MS-AD-BIS (o esquema preferido para a maioria dos servidores AD do Windows 2012 e posteriores)
- Ad-IDMU (Windows 2008, Windows 2016 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)
- RFC-2307 (SERVIDORES LDAP UNIX)

É melhor usar os esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão e modificando a cópia. Para obter mais informações, consulte:

- "Configuração NFS"
- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"

Antes de começar

- Você precisa ter instalado a "Certificado digital do servidor assinado pela CA"no SVM.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Criar uma configuração de cliente LDAP em uma SVM:

`vserver services name-service ldap client create -vserver <SVM_name> -client -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema> -use-start-tls <true|false>`

> Iniciar TLS é compatível apenas para acesso a SVMs de dados. Ele não é compatível com acesso a SVMs administrativas.

Para obter a sintaxe de comando completa, consulte "folha de trabalho".

O comando a seguir cria uma configuração de cliente LDAP chamada `corp` em SVM `engData`. O cliente faz ligações anônimas aos servidores LDAP com os endereços IP 172.160.0.100 e 172.16.0.101. O cliente usa o esquema RFC-2307 para fazer consultas LDAP. A comunicação entre o cliente e o servidor é criptografada usando Iniciar TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

> A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

2. Associe a configuração do cliente LDAP à SVM: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir associa a configuração do cliente LDAP `corp` ao SVM `engData` e habilita o cliente LDAP no SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

   > A partir do ONTAP 9.2, o `vserver services name-service ldap create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

3. Valide o status dos servidores de nomes usando o comando de verificação ldap do serviço de nomes dos serviços vserver.

   O comando a seguir valida servidores LDAP no SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                    |
```

O comando name Service check está disponível a partir de ONTAP 9.2.

Configurar o acesso ao servidor NIS

Você deve configurar o acesso do servidor NIS a um SVM antes que as contas NIS possam acessar o SVM. Você pode usar o `vserver services name-service nis-domain create` comando para criar uma configuração de domínio NIS em um SVM.

Antes de começar

- Todos os servidores configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Crie uma configuração de domínio NIS em uma SVM:

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   > A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

   O comando a seguir cria uma configuração de domínio NIS no SVM `engData`. O domínio NIS `nisdomain` comunica com um servidor NIS com o endereço IP `192.0.2.180` .

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

Crie um switch de serviço de nomes

O recurso de switch de serviço de nomes permite que você use LDAP ou NIS como fontes alternativas de serviço de nomes. Você pode usar o `vserver services name-service ns-switch modify` comando para especificar a ordem de pesquisa para fontes de serviço de nome.

Antes de começar

- Tem de ter configurado o acesso ao servidor LDAP e NIS.

- Você deve ser um administrador de cluster ou um administrador de SVM para executar essa tarefa.

Passo

1. Especifique a ordem de pesquisa para fontes do serviço de nomes:

   `vserver services name-service ns-switch modify -vserver <SVM_name> -database <name_service_switch_database> -sources <name_service_source_order>`

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir especifica a ordem de pesquisa das fontes de serviço de nomes LDAP e NIS para o `passwd` banco de dados no SVM `engData`.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

Altere uma senha de administrador no ONTAP

Você deve alterar sua senha inicial imediatamente após fazer login no sistema pela primeira vez. Se você for um administrador SVM, poderá usar o `security login password` comando para alterar sua própria senha. Se for um administrador de cluster, pode utilizar o `security login password` comando para alterar a palavra-passe de qualquer administrador.

Sobre esta tarefa

A nova palavra-passe deve respeitar as seguintes regras:

- Não pode conter o nome de utilizador
- Deve ter pelo menos oito carateres
- Deve conter pelo menos uma letra e um número
- Não pode ser o mesmo que as últimas seis senhas

> Você pode usar o[`security login role config modify` comando para modificar as regras de senha para contas associadas a uma determinada função. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-role-config-modify.html[`security login role config modify` em referência de comando ONTAP.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para alterar sua própria senha.
- Você deve ser um administrador de cluster para alterar a senha de outro administrador.

Passo

1. Alterar uma palavra-passe de administrador: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   O comando a seguir altera a senha do administrador `admin1` do SVM`vs1.example.com`. É-lhe pedido que introduza a palavra-passe atual e, em seguida, introduza e volte a introduzir a nova palavra-passe.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Bloquear e desbloquear uma conta de administrador

Você pode usar o `security login lock` comando para bloquear uma conta de administrador e o `security login unlock` comando para desbloquear a conta.

Antes de começar

Você deve ser um administrador de cluster para executar essas tarefas.

Passos

1. Bloquear uma conta de administrador:

   `security login lock -vserver SVM_name -username user_name`

   O comando a seguir bloqueia a conta de administrador `admin1` do SVM `vs1.example.com`:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

2. Desbloquear uma conta de administrador:

   `security login unlock -vserver SVM_name -username user_name`

   O comando a seguir desbloqueia a conta de administrador `admin1` do SVM `vs1.example.com`:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

Gerir tentativas de início de sessão falhadas

Tentativas repetidas de login falhadas às vezes indicam que um intruso está tentando acessar o sistema de armazenamento. Você pode executar várias etapas para garantir que não ocorra uma intrusão.

Como você saberá que as tentativas de login falharam

O sistema de Gestão de Eventos (EMS) notifica-o sobre tentativas falhadas de início de sessão a cada hora. Pode encontrar um registo de tentativas de início de sessão falhadas `audit.log` no ficheiro.

O que fazer se tentativas repetidas de login falharem

A curto prazo, você pode executar várias etapas para evitar uma intrusão:

- Exigir que as senhas sejam compostas por um número mínimo de carateres maiúsculos, minúsculos, carateres especiais e/ou dígitos
- Impor um atraso após uma tentativa de início de sessão com falha
- Limite o número de tentativas de início de sessão falhadas permitidas e bloqueie os utilizadores após o número especificado de tentativas falhadas
- Expire e bloqueie contas que estejam inativas por um determinado número de dias

Você pode usar o `security login role config modify` comando para executar essas tarefas.

A longo prazo, você pode seguir estes passos adicionais:

- Use o `security ssh modify` comando para limitar o número de tentativas de login falhadas para todos os SVMs recém-criados.
- Migre contas de algoritmo MD5 existentes para o algoritmo SHA-512 mais seguro, exigindo que os usuários alterem suas senhas.

Aplicar SHA-2 em senhas de conta de administrador

As contas de administrador criadas antes do ONTAP 9.0 continuam a usar senhas MD5 após a atualização, até que as senhas sejam alteradas manualmente. O MD5 é menos seguro do que o SHA-2. Portanto, após a atualização, você deve solicitar aos usuários de contas MD5 que alterem suas senhas para usar a função hash SHA-512 padrão.

Sobre esta tarefa

A funcionalidade hash de senha permite que você faça o seguinte:

- Exibir contas de usuário que correspondem à função hash especificada.
- Expire contas que usam uma função hash especificada (por exemplo, MD5), forçando os usuários a alterar suas senhas em seu próximo login.
- Bloquear contas cujas senhas usam a função hash especificada.
- Ao reverter para uma versão anterior ao ONTAP 9, redefina a própria senha do administrador do cluster para que ela seja compatível com a função hash (MD5) que é suportada pela versão anterior.

O ONTAP aceita senhas SHA-2 pré-hash somente usando o SDK de gerenciamento do NetApp (`security-login-create`e `security-login-modify-password`o).

Passos

1. Migre as contas de administrador do MD5 para a função hash de senha SHA-512:
   a. Expire todas as contas de administrador do MD5: `security login expire-password -vserver * -username * -hash-function md5`

      Isso força os usuários de conta do MD5 a alterar suas senhas no próximo login.

   b. Peça aos usuários de contas do MD5 para fazer login por meio de um console ou sessão SSH.

      O sistema deteta que as contas estão expiradas e solicita aos usuários que alterem suas senhas. Sha-512 é usado por padrão para as senhas alteradas.
2. Para contas do MD5 cujos usuários não fazem login para alterar suas senhas dentro de um período de

tempo, force a migração da conta:

a. Bloquear contas que ainda usam a função hash MD5 (nível de privilégio avançado): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

   Após o número de dias especificado pelo `-lock-after`, os usuários não podem acessar suas contas do MD5.

b. Desbloqueie as contas quando os usuários estiverem prontos para alterar suas senhas: `security login unlock -vserver svm_name -username user_name`

c. Faça com que os usuários façam login em suas contas por meio de uma sessão de console ou SSH e alterem suas senhas quando o sistema solicitar que façam isso.

Diagnosticar e corrigir problemas de acesso a arquivos

Passos

1. No System Manager, selecione **Storage > Storage VMs**.
2. Selecione a VM de armazenamento na qual você deseja executar um rastreamento.
3. Clique ⋮ em **mais**.
4. Clique em **Trace File Access**.
5. Forneça o nome de usuário e o endereço IP do cliente e clique em **Iniciar rastreamento**.

   Os resultados do rastreio são apresentados numa tabela. A coluna **razões** fornece o motivo pelo qual um arquivo não pôde ser acessado.

6. Clique ⌄ na coluna esquerda da tabela de resultados para visualizar as permissões de acesso ao arquivo.

Gerenciar a verificação de vários administradores

Visão geral da verificação de vários administradores do ONTAP

A partir do ONTAP 9.11,1, você pode usar a verificação multiadministrador (MAV) para garantir que certas operações, como a exclusão de volumes ou cópias Snapshot, possam ser executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

A configuração da verificação de vários administradores consiste em:

- "Criando um ou mais grupos de aprovação de administrador."
- "Habilitando a funcionalidade de verificação de vários administradores."
- "Adicionar ou modificar regras."

Após a configuração inicial, esses elementos só podem ser modificados por administradores em um grupo de aprovação MAV (administradores MAV).

Quando a verificação multi-admin está ativada, a conclusão de cada operação protegida requer estes passos:

1. Quando um utilizador inicia a operação, a "a solicitação é gerada."
2. Antes que a operação possa ser executada, pelo menos uma "O administrador do MAV deve aprovar."
3. Após a aprovação, o usuário é solicitado e conclui a operação.

> Se você precisar desabilitar a funcionalidade de verificação multiadministrador sem a aprovação do administrador do MAV, entre em Contato com o suporte da NetApp e mencione o seguinte artigo da base de dados de Conhecimento: "Como desativar a Verificação Multi-Admin se o administrador do MAV não estiver disponível".

A verificação multiadministrador não se destina a ser usada com volumes ou fluxos de trabalho que envolvam automação pesada, pois cada tarefa automatizada exigiria aprovação antes que a operação pudesse ser concluída. Se você quiser usar automação e MAV juntos, é recomendável usar consultas para operações MAV específicas. Por exemplo, você pode aplicar `volume delete` regras MAV apenas a volumes em que a automação não está envolvida e pode designar esses volumes com um esquema de nomenclatura específico.

> A verificação multi-admin não está disponível com o Cloud Volumes ONTAP.

Como a verificação multi-admin funciona

A verificação multi-admin consiste em:

- Um grupo de um ou mais administradores com poderes de aprovação e veto.
- Um conjunto de operações ou comandos protegidos em uma tabela *rules*.
- Um mecanismo *regras* para identificar e controlar a execução de operações protegidas.

As regras MAV são avaliadas após regras de controle de acesso baseado em função (RBAC). Portanto, os administradores que executam ou aprovam operações protegidas já devem possuir o Privileges RBAC mínimo para essas operações. "Saiba mais sobre o RBAC".

Regras definidas pelo sistema

Quando a verificação multi-admin está ativada, as regras definidas pelo sistema (também conhecidas como regras *guard-rail*) estabelecem um conjunto de operações MAV para conter o risco de contornar o próprio processo MAV. Essas operações não podem ser removidas da tabela de regras. Quando o MAV estiver ativado, as operações designadas por um asterisco (*) requerem aprovação por um ou mais administradores antes da execução, exceto para os comandos **show**.

- `security multi-admin-verify modify` operação `*`

  Controla a configuração da funcionalidade de verificação de vários administradores.

- `security multi-admin-verify approval-group` operações `*`

  Controle a associação no conjunto de administradores com credenciais de verificação multi-admin.

- `security multi-admin-verify rule` operações `*`

  Controle o conjunto de comandos que exigem verificação multi-admin.

- `security multi-admin-verify request` operações

  Controle o processo de aprovação.

Comandos protegidos por regras

Além das operações definidas pelo sistema, os seguintes comandos são protegidos por padrão quando a verificação multi-admin está ativada, mas você pode modificar as regras para remover a proteção desses comandos.

- `security login password`
- `security login unlock`
- `set`

Cada versão do ONTAP fornece mais comandos que você pode escolher para proteger com regras de verificação de vários administradores. Escolha a versão do ONTAP para obter a lista completa de comandos disponíveis para proteção.

9.16.1

- `cluster date modify` 3
- `cluster log-forwarding create` 3
- `cluster log-forwarding delete` 3
- `cluster log-forwarding modify` 3
- `cluster peer delete`
- `cluster time-service ntp server create` 3
- `cluster time-service ntp server delete` 3
- `cluster time-service ntp server key create` 3
- `cluster time-service ntp server key delete` 3
- `cluster time-service ntp server key modify` 3
- `cluster time-service ntp server modify` 3
- `event config modify`
- `lun delete` 3
- `security anti-ransomware volume attack clear-suspect` 1
- `security anti-ransomware volume disable` 1
- `security anti-ransomware volume event-log modify` 2
- `security anti-ransomware volume pause` 1
- `security anti-ransomware vserver event-log modify` 2
- `security audit modify` 3
- `security ipsec config modify` 3
- `security ipsec policy create` 3
- `security ipsec policy delete` 3
- `security ipsec policy modify` 3
- `security login create`
- `security login delete`
- `security login modify`
- `security key-manager onboard update-passphrase` 3
- `security saml-sp create` 3
- `security saml-sp delete` 3
- `security saml-sp modify` 3
- `snaplock legal-hold end` 3
- `storage aggregate delete` 3

- storage aggregate offline 4
- storage encryption disk destroy 3
- storage encryption disk modify 3
- storage encryption disk revert-to-original-state 3
- storage encryption disk sanitize 3
- system bridge run-cli 3
- system controller flash-cache secure-erase run 3
- system controller service-event delete 3
- system health alert delete 3
- system health alert modify 3
- system health policy definition modify 3
- system node autosupport modify 3
- system node autosupport trigger modify 3
- system node coredump delete 3
- system node coredump delete-all 3
- system node hardware nvram-encryption modify 3
- system node run
- system node systemshell
- system script delete 3
- system service-processor ssh add-allowed-addresses 3
- system service-processor ssh remove-allowed-addresses 3
- system smtape restore 3
- system switch ethernet log disable-collection 3
- system switch ethernet log modify 3
- timezone 3
- volume create 3
- volume delete
- volume encryption conversion start 4
- volume encryption rekey start 4
- volume file privileged-delete 3
- volume flexcache delete
- volume modify 3
- volume recovery-queue modify 2
- volume recovery-queue purge 2

- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot create 3
- volume snapshot delete
- volume snapshot modify 3
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename 3
- volume snapshot restore
- vserver audit create 3
- vserver audit delete 3
- vserver audit disable 3
- vserver audit modify 3
- vserver audit rotate-log 3
- vserver create 2
- vserver consistency-group create 4
- vserver consistency-group delete 4
- vserver consistency-group modify 4
- vserver consistency-group snapshot create 4
- vserver consistency-group snapshot delete 4
- vserver delete 3
- vserver modify 2
- vserver object-store-server audit create 3
- vserver object-store-server audit delete 3
- vserver object-store-server audit disable 3
- vserver object-store-server audit modify 3
- vserver object-store-server audit rotate-log 3
- vserver options 3
- vserver peer delete

- vserver security file-directory apply 3
- vserver security file-directory remove-slag 3
- vserver stop 4
- vserver vscan disable 3
- vserver vscan on-access-policy create 3
- vserver vscan on-access-policy delete 3
- vserver vscan on-access-policy disable 3
- vserver vscan on-access-policy modify 3
- vserver vscan scanner-pool create 3
- vserver vscan scanner-pool delete 3
- vserver vscan scanner-pool modify 3

9.15.1

- cluster date modify 3
- cluster log-forwarding create 3
- cluster log-forwarding delete 3
- cluster log-forwarding modify 3
- cluster peer delete
- cluster time-service ntp server create 3
- cluster time-service ntp server delete 3
- cluster time-service ntp server key create 3
- cluster time-service ntp server key delete 3
- cluster time-service ntp server key modify 3
- cluster time-service ntp server modify 3
- event config modify
- lun delete 3
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume event-log modify 2
- security anti-ransomware volume pause 1
- security anti-ransomware vserver event-log modify 2
- security audit modify 3
- security ipsec config modify 3
- security ipsec policy create 3

- security ipsec policy delete 3
- security ipsec policy modify 3
- security login create
- security login delete
- security login modify
- security key-manager onboard update-passphrase 3
- security saml-sp create 3
- security saml-sp delete 3
- security saml-sp modify 3
- snaplock legal-hold end 3
- storage aggregate delete 3
- storage encryption disk destroy 3
- storage encryption disk modify 3
- storage encryption disk revert-to-original-state 3
- storage encryption disk sanitize 3
- system bridge run-cli 3
- system controller flash-cache secure-erase run 3
- system controller service-event delete 3
- system health alert delete 3
- system health alert modify 3
- system health policy definition modify 3
- system node autosupport modify 3
- system node autosupport trigger modify 3
- system node coredump delete 3
- system node coredump delete-all 3
- system node hardware nvram-encryption modify 3
- system node run
- system node systemshell
- system script delete 3
- system service-processor ssh add-allowed-addresses 3
- system service-processor ssh remove-allowed-addresses 3
- system smtape restore 3
- system switch ethernet log disable-collection 3
- system switch ethernet log modify 3

- timezone 3
- volume create 3
- volume delete
- volume file privileged-delete 3
- volume flexcache delete
- volume modify 3
- volume recovery-queue modify 2
- volume recovery-queue purge 2
- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot create 3
- volume snapshot delete
- volume snapshot modify 3
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename 3
- volume snapshot restore
- vserver audit create 3
- vserver audit delete 3
- vserver audit disable 3
- vserver audit modify 3
- vserver audit rotate-log 3
- vserver create 2
- vserver delete 3
- vserver modify 2
- vserver object-store-server audit create 3
- vserver object-store-server audit delete 3
- vserver object-store-server audit disable 3
- vserver object-store-server audit modify 3

- vserver object-store-server audit rotate-log 3
- vserver options 3
- vserver peer delete
- vserver security file-directory apply 3
- vserver security file-directory remove-slag 3
- vserver vscan disable 3
- vserver vscan on-access-policy create 3
- vserver vscan on-access-policy delete 3
- vserver vscan on-access-policy disable 3
- vserver vscan on-access-policy modify 3
- vserver vscan scanner-pool create 3
- vserver vscan scanner-pool delete 3
- vserver vscan scanner-pool modify 3

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume event-log modify 2
- security anti-ransomware volume pause 1
- security anti-ransomware vserver event-log modify 2
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify 2
- volume recovery-queue purge 2
- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify

- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create 2
- vserver modify 2
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume pause 1
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule

- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

1. Novo comando protegido por regras para 9.13.1
2. Novo comando protegido por regras para 9.14.1
3. Novo comando protegido por regras para 9.15.1
4. Novo comando protegido por regras para 9.16.1

*Este comando só está disponível com CLI e não está disponível para o System Manager em algumas versões.

Como funciona a aprovação multi-admin

Sempre que uma operação protegida é inserida em um cluster protegido por MAV, uma solicitação de execução de operação é enviada para o grupo de administradores designado MAV.

Você pode configurar:

- Nomes, informações de Contato e número de administradores no grupo MAV.

Um administrador MAV deve ter uma função RBAC com o administrador de cluster Privileges.

- O número de grupos de administradores do MAV.
  - Um grupo MAV é atribuído para cada regra de operação protegida.
  - Para vários grupos MAV, você pode configurar qual grupo MAV aprova uma determinada regra.
- O número de aprovações MAV necessárias para executar uma operação protegida.
- Um período de expiração de *aprovação* dentro do qual um administrador do MAV deve responder a uma solicitação de aprovação.
- Um período de expiração de *execução* dentro do qual o administrador solicitante deve concluir a operação.

Uma vez configurados esses parâmetros, a aprovação MAV é necessária para modificá-los.

Os administradores do MAV não podem aprovar suas próprias solicitações para executar operações protegidas. Por conseguinte:

- O MAV não deve ser ativado em clusters com apenas um administrador.
- Se houver apenas uma pessoa no grupo MAV, o administrador do MAV não poderá iniciar operações protegidas; os administradores regulares devem iniciar operações protegidas e o administrador do MAV só pode aprovar.
- Se você quiser que os administradores do MAV possam executar operações protegidas, o número de administradores do MAV deve ser maior do que o número de aprovações necessárias. Por exemplo, se duas aprovações forem necessárias para uma operação protegida e você quiser que os administradores do MAV as executem, deve haver três pessoas no grupo de administradores do MAV.

Os administradores do MAV podem receber solicitações de aprovação em alertas de e-mail (usando o EMS) ou podem consultar a fila de solicitações. Quando recebem um pedido, podem tomar uma das três ações:

- Aprovar
- Rejeitar (veto)
- Ignorar (sem ação)

As notificações por e-mail são enviadas a todos os aprovadores associados a uma regra MAV quando:

- Uma solicitação é criada.
- Uma solicitação é aprovada ou vetada.
- Uma solicitação aprovada é executada.

Se o solicitante estiver no mesmo grupo de aprovação para a operação, ele receberá um e-mail quando a solicitação for aprovada.

> Um solicitante não pode aprovar suas próprias solicitações, mesmo que esteja no grupo de aprovação (embora possa receber notificações por e-mail para suas próprias solicitações). Os solicitantes que não estão em grupos de aprovação (ou seja, que não são administradores MAV) não recebem notificações por e-mail.

Como funciona a execução da operação protegida

Se a execução for aprovada para uma operação protegida, o usuário solicitante continuará com a operação

quando solicitado. Se a operação for vetada, o usuário solicitante deverá excluir a solicitação antes de prosseguir.

As regras MAV são avaliadas após as permissões RBAC. Como resultado, um usuário sem permissões RBAC suficientes para execução da operação não pode iniciar o processo de solicitação MAV.

Gerenciar grupos de aprovação de administrador

Antes de ativar a verificação multi-admin (MAV), você deve criar um grupo de aprovação de administrador contendo um ou mais administradores para receber autoridade de aprovação ou veto. Depois de ativar a verificação multi-admin, quaisquer modificações na associação ao grupo de aprovação requerem a aprovação de um dos administradores qualificados existentes.

Sobre esta tarefa

Você pode adicionar administradores existentes a um grupo MAV ou criar novos administradores.

A funcionalidade MAV homenageia as configurações de controle de acesso baseado em função (RBAC) existentes. Os potenciais administradores do MAV devem ter privilégios suficientes para executar operações protegidas antes de serem adicionados aos grupos de administradores do MAV. "Saiba mais sobre o RBAC."

Você pode configurar o MAV para alertar os administradores do MAV de que as solicitações de aprovação estão pendentes. Para fazer isso, você deve configurar notificações por e-mail - em particular, os `Mail From` parâmetros e `Mail Server` - ou você pode limpar esses parâmetros para desativar a notificação. Sem alertas de e-mail, os administradores do MAV devem verificar a fila de aprovação manualmente.

Procedimento do System Manager

Se pretender criar um grupo de aprovação MAV pela primeira vez, consulte o procedimento do Gestor do sistema para "ative a verificação de vários administradores."

Para modificar um grupo de aprovação existente ou criar um grupo de aprovação adicional:

1. Identifique os administradores para receber a verificação de vários administradores.
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **usuários e funções.**
   c. Clique + Add em **Users.**
   d. Modifique a lista conforme necessário.

      Para obter mais informações, consulte "Controle o acesso do administrador."

2. Criar ou modificar o grupo de aprovação MAV:
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **aprovação Multi-Admin** na seção **Segurança**. (Você verá o ⚙ ícone se o MAV ainda não estiver configurado.)
      - Nome: Introduza um nome de grupo.
      - Aprovadores: Selecione aprovadores de uma lista de usuários.
      - Endereço de e-mail: Insira o(s) endereço(s) de e-mail.
      - Grupo padrão: Selecione um grupo.

A aprovação MAV é necessária para editar uma configuração existente assim que o MAV estiver ativado.

Procedimento CLI

1. Verifique se os valores foram definidos para `Mail From` os parâmetros e. `Mail Server` Introduza:

   `event config show`

   O visor deve ser semelhante ao seguinte:

   ```
   cluster01::> event config show
                              Mail From:  admin@localhost
                            Mail Server:  localhost
                              Proxy URL:  -
                             Proxy User:  -
    Publish/Subscribe Messaging Enabled:  true
   ```

   Para configurar estes parâmetros, introduza:

   `event config modify -mail-from` *`email_address`* `-mail-server` *`server_name`*

2. Identifique os administradores para receber a verificação de vários administradores

Se você quiser…	Introduza este comando
Exibir administradores atuais	`security login show`
Modifique as credenciais dos administradores atuais	`security login modify <parameters>`
Crie novas contas de administrador	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

3. Crie o grupo de aprovação MAV:

   `security multi-admin-verify approval-group create [ -vserver` *`svm_name`*`] -name` *`group_name`* `-approvers` *`approver1`*`[,`*`approver2`*`…] [[-email` *`address1`*`], `*`address1`*`…]`

   - `-vserver` - Somente o administrador SVM é suportado nesta versão.
   - `-name` - O nome do grupo MAV, até 64 carateres.
   - `-approvers` - A lista de um ou mais aprovadores.
   - `-email` - Um ou mais endereços de e-mail que são notificados quando uma solicitação é criada, aprovada, vetada ou executada.

     Exemplo: o comando a seguir cria um grupo MAV com dois membros e endereços de e-mail associados.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Verificar a criação e a associação do grupo:

   `security multi-admin-verify approval-group show`

   Exemplo:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

Use esses comandos para modificar a configuração inicial do grupo MAV.

Nota: todos exigem aprovação do administrador do MAV antes da execução.

Se você quiser…	Introduza este comando
Modifique as caraterísticas do grupo ou modifique as informações de membros existentes	`security multi-admin-verify approval-group modify [`*parameters*`]`
Adicionar ou remover membros	`security multi-admin-verify approval-group replace [-vserver` *svm_name*`] -name` *group_name* `[-approvers-to-add` *approver1*`[,`*approver2*`…]][-approvers-to-remove` *approver1*`[,`*approver2*`…]]`
Eliminar um grupo	`security multi-admin-verify approval-group delete [-vserver` *svm_name*`] -name` *group_name*

Ative e desative a verificação de vários administradores

A verificação multi-admin (MAV) deve ser ativada explicitamente. Depois de ativar a verificação multi-admin, a aprovação por administradores em um grupo de aprovação MAV (administradores MAV) é necessária para excluí-la.

Sobre esta tarefa

Uma vez que o MAV está ativado, modificar ou desativar o MAV requer a aprovação do administrador do MAV.

Se você precisar desabilitar a funcionalidade de verificação multiadministrador sem a aprovação do administrador do MAV, entre em Contato com o suporte da NetApp e mencione o seguinte artigo da base de dados de Conhecimento: "Como desativar a Verificação Multi-Admin se o administrador do MAV não estiver disponível".

Ao ativar o MAV, você pode especificar os seguintes parâmetros globalmente.

Grupos de aprovação

Uma lista de grupos de aprovação globais. É necessário pelo menos um grupo para ativar a funcionalidade MAV.

Se você estiver usando o MAV com o Autonomous ransomware Protection (ARP), defina um grupo de aprovação novo ou existente que seja responsável por aprovar a pausa ARP, desativar e limpar solicitações suspeitas.

Aprovadores necessários

O número de aprovadores necessários para executar uma operação protegida. O número padrão e mínimo é 1.

O número necessário de aprovadores deve ser menor que o número total de aprovadores exclusivos nos grupos de aprovação padrão.

Validade da aprovação (horas, minutos, segundos)

O período durante o qual um administrador do MAV deve responder a uma solicitação de aprovação. O valor padrão é de uma hora (1h), o valor mínimo suportado é de um segundo (1s) e o valor máximo suportado é de 14 dias (14d).

Expiração da execução (horas, minutos, segundos)

O período durante o qual o administrador requerente deve concluir a operação::. O valor padrão é de uma hora (1h), o valor mínimo suportado é de um segundo (1s) e o valor máximo suportado é de 14 dias (14d).

Você também pode substituir qualquer um desses parâmetros para específico "regras de operação."

Procedimento do System Manager

1. Identifique os administradores para receber a verificação de vários administradores.
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **usuários e funções.**
   c. Clique + Add em **Users.**
   d. Modifique a lista conforme necessário.

      Para obter mais informações, consulte "Controle o acesso do administrador."

2. Ative a verificação de vários administradores criando pelo menos um grupo de aprovação e adicionando pelo menos uma regra.
   a. Clique em **Cluster > Settings.**
   b. Clique ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
   c. Clique + Add para adicionar pelo menos um grupo de aprovação.

- Name (Nome) – Introduza o nome de um grupo.
- Aprovadores – Selecione aprovadores de uma lista de usuários.
- Endereço de e-mail – Digite o(s) endereço(s) de e-mail.
- Grupo padrão – Selecione um grupo.

d. Adicione pelo menos uma regra.
   - Operação – Selecione um comando suportado na lista.
   - Consulta – Insira quaisquer opções e valores de comando desejados.
   - Parâmetros opcionais; deixe em branco para aplicar configurações globais ou atribua um valor diferente para regras específicas para substituir as configurações globais.
     - Número necessário de aprovadores
     - Grupos de aprovação
e. Clique em **Configurações avançadas** para exibir ou modificar os padrões.
   - Número necessário de aprovadores (padrão: 1)
   - Expiração da solicitação de execução (padrão: 1 hora)
   - Expiração do pedido de aprovação (predefinição: 1hour)
   - Servidor de correio*
   - A partir do endereço de e-mail*

     *Estes atualizam as definições de e-mail geridas em "Gestão de notificações". Você será solicitado a configurá-los se eles ainda não tiverem sido configurados.
f. Clique em **Enable** para concluir a configuração inicial do MAV.

Após a configuração inicial, o status atual do MAV é exibido no mosaico **aprovação Multi-Admin**.

- Estado (ativado ou não)
- Operações ativas para as quais são necessárias aprovações
- Número de solicitações abertas no estado pendente

Você pode exibir uma configuração existente clicando →em . A aprovação MAV é necessária para editar uma configuração existente.

Para desativar a verificação de vários administradores:

1. Clique em **Cluster > Settings.**
2. Clique ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
3. Clique no botão de alternância ativado.

   A aprovação MAV é necessária para concluir esta operação.

Procedimento CLI

Antes de ativar a funcionalidade MAV na CLI, pelo menos um "Grupo de administradores do MAV"deve ter sido criado.

Se você quiser…	Introduza este comando

Ativar a funcionalidade MAV	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	Exemplo : o comando a seguir habilita o MAV com 1 grupo de aprovação, 2 aprovadores necessários e períodos de expiração padrão.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Conclua a configuração inicial adicionando pelo menos uma "regra de operação."

Modificar uma configuração MAV (requer aprovação MAV)	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

Verifique a funcionalidade MAV	`security multi-admin-verify show`
	
	Exemplo:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- -------- ----------`
	`true 2 1h 1h mav-grp1`

Desativar a funcionalidade MAV (requer aprovação MAV)	`security multi-admin-verify modify -enabled false`

Gerenciar regras de operação protegidas

Você cria regras de verificação multi-admin (MAV) para designar operações que exigem aprovação. Sempre que uma operação é iniciada, operações protegidas são intercetadas e uma solicitação de aprovação é gerada.

As regras podem ser criadas antes de ativar o MAV por qualquer administrador com recursos RBAC apropriados, mas uma vez que o MAV está habilitado, qualquer modificação no conjunto de regras requer aprovação MAV.

Apenas uma regra MAV pode ser criada por operação; por exemplo, você não pode fazer várias `volume-snapshot-delete` regras. Quaisquer restrições de regra desejadas devem estar contidas em uma regra.

Você pode criar regras para proteger "estes comandos". Você pode proteger cada comando começando com a versão ONTAP na qual a capacidade de proteção para o comando ficou disponível pela primeira vez.

As regras para os comandos padrão do sistema MAV, o `security multi-admin-verify` "comandos", não podem ser alteradas.

Além das operações definidas pelo sistema, os seguintes comandos são protegidos por padrão quando a verificação multi-admin está ativada, mas você pode modificar as regras para remover a proteção desses comandos.

- `security login password`
- `security login unlock`
- `set`

Restrições de regra

Ao criar uma regra, você pode especificar opcionalmente a `-query` opção para limitar a solicitação a um subconjunto da funcionalidade de comando. A `-query` opção também pode ser usada para limitar elementos de configuração, como SVM, volume e nomes de Snapshot.

Por exemplo, no `volume snapshot delete` comando, `-query` pode ser definido como `-snapshot !hourly*,!daily*,!weekly*`, o que significa que instantâneos de volume pré-fixados com atributos de hora em hora, dia ou semanal são excluídos das proteções MAV.

```
smci-vsim20::> security multi-admin-verify rule show
                                                Required  Approval
Vserver Operation                               Approvers Groups
------- --------------------------------------- --------- -------------
vs01    volume snapshot delete                  -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

Quaisquer elementos de configuração excluídos não seriam protegidos pelo MAV, e qualquer administrador poderia excluí-los ou renomeá-los.

Por padrão, as regras especificam que um comando correspondente `security multi-admin-verify request create "protected_operation"` é gerado automaticamente quando uma operação protegida

é inserida. Você pode modificar esse padrão para exigir que o `request create` comando seja inserido separadamente.

Por padrão, as regras herdam as seguintes configurações globais de MAV, embora você possa especificar exceções específicas de regras:

- Número necessário de Aprovadores
- Grupos de aprovação
- Período de validade da aprovação
- Período de expiração da execução

Procedimento do System Manager

Se pretender adicionar uma regra de operação protegida pela primeira vez, consulte o procedimento do Gestor de sistema a. "ative a verificação de vários administradores."

Para modificar o conjunto de regras existente:

1. Selecione **Cluster > Settings**.
2. Selecione ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
3. + Add Selecione para adicionar pelo menos uma regra; você também pode modificar ou excluir regras existentes.
   - Operação – Selecione um comando suportado na lista.
   - Consulta – Insira quaisquer opções e valores de comando desejados.
   - Parâmetros opcionais – deixe em branco para aplicar configurações globais ou atribua um valor diferente para regras específicas para substituir as configurações globais.
     - Número necessário de aprovadores
     - Grupos de aprovação

Procedimento CLI

ⓘ Todos `security multi-admin-verify rule` os comandos requerem aprovação do administrador MAV antes da execução, exceto `security multi-admin-verify rule show`.

Se você quiser…	Introduza este comando
Crie uma regra	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Se você quiser…	Introduza este comando

Modifique as credenciais dos administradores atuais	`security login modify <parameters>`
	
	Exemplo: A regra a seguir requer aprovação para excluir o volume raiz.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modificar uma regra	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Excluir uma regra	`security multi-admin-verify rule delete -operation "protected_operation"`
Mostrar regras	`security multi-admin-verify rule show`

Para obter detalhes da sintaxe do comando, consulte as `security multi-admin-verify rule` páginas man.

Solicitar a execução de operações protegidas

Quando você inicia uma operação ou comando protegidos em um cluster habilitado para verificação multi-admin (MAV), o ONTAP interceta automaticamente a operação e solicita a geração de uma solicitação, que deve ser aprovada por um ou mais administradores em um grupo de aprovação MAV (administradores MAV). Alternativamente, você pode criar uma solicitação MAV sem a caixa de diálogo.

Se aprovado, você deve responder à consulta para concluir a operação dentro do período de expiração da solicitação. Se vetado, ou se a solicitação ou os períodos de expiração forem excedidos, você deverá excluir a solicitação e reenviar.

A funcionalidade MAV homenageia as configurações RBAC existentes. Ou seja, sua função de administrador deve ter privilégio suficiente para executar uma operação protegida sem considerar as configurações de MAV. "Saiba mais sobre o RBAC".

Se você for um administrador do MAV, suas solicitações para executar operações protegidas também devem ser aprovadas por um administrador do MAV.

Procedimento do System Manager

Quando um usuário clica em um item de menu para iniciar uma operação e a operação é protegida, uma solicitação de aprovação é gerada e o usuário recebe uma notificação semelhante à seguinte:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

A janela **pedidos Multi-Admin** está disponível quando o MAV está ativado, mostrando solicitações pendentes com base no ID de login do usuário e na função MAV (aprovador ou não). Para cada solicitação pendente, os seguintes campos são exibidos:

- Operação
- Índice (número)
- Estado (pendente, aprovado, rejeitado, executado ou expirado)

  Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

- Consulta (quaisquer parâmetros ou valores para a operação solicitada)
- Utilizador a solicitar
- A solicitação expira em
- (Número de) Aprovadores pendentes
- (Número de) potenciais Aprovadores

Quando a solicitação for aprovada, o usuário solicitante poderá tentar novamente a operação dentro do período de expiração.

Se o utilizador voltar a tentar a operação sem aprovação, é apresentada uma notificação semelhante à seguinte:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

Procedimento CLI

1. Introduzir diretamente a operação protegida ou através do comando pedido MAV.

   Exemplos – para excluir um volume, digite um dos seguintes comandos:

   ◦ `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create “volume delete”`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. Verifique o status da solicitação e responda ao aviso MAV.
   a. Se a solicitação for aprovada, responda à mensagem CLI para concluir a operação.

      Exemplo:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. Se a solicitação for vetada ou se o período de expiração tiver passado, exclua a solicitação e envie novamente ou entre em Contato com o administrador do MAV.

Exemplo:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gerenciar solicitações de operação protegidas

Quando os administradores de um grupo de aprovação MAV (administradores MAV) são notificados de uma solicitação de execução de operação pendente, eles devem responder com uma mensagem de aprovação ou veto dentro de um período de tempo fixo (expiração da aprovação). Se um número suficiente de aprovações não for recebido, o solicitante deve excluir a solicitação e fazer outra.

Sobre esta tarefa

As solicitações de aprovação são identificadas com números de índice, que são incluídos em mensagens de e-mail e exibições da fila de solicitações.

As seguintes informações da fila de pedidos podem ser exibidas:

Operação
A operação protegida para a qual a solicitação é criada.

Consulta
O objeto (ou objetos) sobre o qual o usuário deseja aplicar a operação.

Estado

O estado atual da solicitação; pendente, aprovado, rejeitado, expirado, executado. Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

Aprovadores necessários

O número de administradores MAV que são necessários para aprovar a solicitação. Um usuário pode definir o parâmetro de aprovadores necessários para a regra de operação. Se um usuário não definir os aprovadores necessários para a regra, os aprovadores necessários da configuração global serão aplicados.

Aprovadores pendentes

O número de administradores MAV que ainda são obrigados a aprovar a solicitação para que a solicitação seja marcada como aprovada.

Validade da aprovação

O período durante o qual um administrador do MAV deve responder a uma solicitação de aprovação. Qualquer utilizador autorizado pode definir a validade da aprovação para uma regra de operação. Se a expiração da aprovação não for definida para a regra, então a expiração da aprovação do ajuste global é aplicada.

Expiração da execução

O período durante o qual o administrador requerente deve concluir a operação. Qualquer usuário autorizado pode definir a expiração de execução para uma regra de operação. Se a execução-expiração não estiver definida para a regra, então a execução-expiração da configuração global será aplicada.

Usuários aprovados

Os administradores do MAV que aprovaram a solicitação.

Vetado pelo utilizador

Os administradores do MAV que vetaram a solicitação.

VM de storage (vserver)

O SVM com o qual a solicitação está associada. Somente o SVM admin é compatível nesta versão.

Utilizador solicitado

O nome de usuário do usuário que criou a solicitação.

Hora criada

A hora em que a solicitação é criada.

Hora aprovada

A hora em que o estado da solicitação foi alterado para aprovado.

Comentário

Quaisquer comentários associados à solicitação.

Usuários permitidos

A lista de utilizadores autorizados a realizar a operação protegida para a qual a solicitação foi aprovada. Se `users-permitted` estiver vazio, qualquer usuário com permissões apropriadas pode executar a operação.

Todas as solicitações expiradas ou executadas são excluídas quando um limite de 1000 solicitações é atingido

ou quando o tempo expirado é maior que 8hrs para solicitações expiradas. As solicitações vetadas são excluídas depois que forem marcadas como expiradas.

Procedimento do System Manager

Os administradores do MAV recebem mensagens de e-mail com detalhes da solicitação de aprovação, período de expiração da solicitação e um link para aprovar ou rejeitar a solicitação. Eles podem acessar uma caixa de diálogo de aprovação clicando no link no e-mail ou navegar para **Eventos & trabalhos>solicitações** no System Manager.

A janela **Requests** está disponível quando a verificação multi-admin está ativada, mostrando solicitações pendentes com base no ID de login do usuário e na função MAV (aprovador ou não).

- Operação
- Índice (número)
- Estado (pendente, aprovado, rejeitado, executado ou expirado)

  Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

- Consulta (quaisquer parâmetros ou valores para a operação solicitada)
- Utilizador a solicitar
- A solicitação expira em
- (Número de) Aprovadores pendentes
- (Número de) potenciais Aprovadores

Os administradores do MAV têm controles adicionais nesta janela; eles podem aprovar, rejeitar ou excluir operações individuais ou grupos selecionados de operações. No entanto, se o administrador MAV for o Usuário solicitante, ele não poderá aprovar, rejeitar ou excluir seus próprios pedidos.

Procedimento CLI

1. Quando notificado de solicitações pendentes por e-mail, observe o número de índice e o período de expiração da aprovação da solicitação. O número do índice também pode ser exibido usando as opções **show** ou **show-pending** mencionadas abaixo.
2. Aprovar ou vetar o pedido.

Se você quiser…	Introduza este comando
Aprovar uma solicitação	`security multi-admin-verify request approve` *nn*
Veto um pedido	`security multi-admin-verify request veto` *nn*
Mostrar todas as solicitações, solicitações pendentes ou uma única solicitação	`security multi-admin-verify request { show

Se você quiser…	Introduza este comando
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Você pode mostrar todas as solicitações na fila ou apenas solicitações pendentes. Se introduzir o número do índice, apenas são apresentadas informações para esse número. Você pode exibir informações sobre campos específicos (usando o `-fields` parâmetro) ou sobre todos os campos (usando o `-instance` parâmetro).
Eliminar um pedido	`security multi-admin-verify request delete` *nn*

Exemplo:

A sequência a seguir aprova uma solicitação após o administrador do MAV receber o e-mail da solicitação com o índice número 3, que já tem uma aprovação.

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Exemplo:

A sequência a seguir veta uma solicitação depois que o administrador do MAV recebeu o e-mail da solicitação com o índice número 3, que já tem uma aprovação.

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Gerenciar autorização dinâmica

Descrição geral da autorização dinâmica

A partir do ONTAP 9.15,1, os administradores podem configurar e habilitar a autorização dinâmica para aumentar a segurança do acesso remoto ao ONTAP, além de mitigar possíveis danos que podem ser causados por um ator mal-intencionado. Com o ONTAP 9.15,1, a autorização dinâmica fornece uma estrutura inicial para atribuir uma pontuação de segurança aos usuários e, se sua atividade parecer suspeita, desafiando-os com verificações de autorização adicionais ou negando uma operação completamente. Os administradores podem criar regras, atribuir pontuações de confiança e restringir comandos para determinar quando determinada atividade é permitida ou negada para um usuário. Os administradores podem habilitar a autorização dinâmica em todo o

cluster ou para VMs de armazenamento individuais.

Como funciona a autorização dinâmica

A autorização dinâmica utiliza um sistema de pontuação de confiança para atribuir aos utilizadores um nível de confiança diferente, dependendo das políticas de autorização. Com base no nível de confiança do usuário, uma atividade que ele executa pode ser permitida ou negada, ou o usuário pode ser solicitado para autenticação adicional.

"Personalizar autorização dinâmica"Consulte para saber mais sobre como configurar pesos de pontuação de critérios e outros atributos de autorização dinâmica.

Dispositivos confiáveis

Quando a autorização dinâmica está em uso, a definição de um dispositivo confiável é um dispositivo usado por um usuário para fazer login no ONTAP usando autenticação de chave pública como um dos métodos de autenticação. O dispositivo é confiável porque somente esse usuário possui a chave privada correspondente.

Exemplo de autorização dinâmica

Veja o exemplo de três usuários diferentes tentando excluir um volume. Quando eles tentam executar a operação, a classificação de risco para cada usuário é examinada:

- O primeiro usuário faz login de um dispositivo confiável com poucas falhas de autenticação anteriores, o que torna sua classificação de risco baixa; a operação é permitida sem autenticação adicional.
- O segundo usuário faz login em um dispositivo confiável com uma porcentagem moderada de falhas de autenticação anteriores, o que torna a classificação de risco moderada; ela é solicitada a autenticação adicional antes que a operação seja permitida.
- O terceiro usuário faz logon de um dispositivo não confiável com uma alta porcentagem de falhas de autenticação anteriores, o que torna a classificação de risco alta; a operação não é permitida.

O que vem a seguir

- "Ativar ou desativar a autorização dinâmica"
- "Personalizar autorização dinâmica"

Ative ou desative a autorização dinâmica no ONTAP

A partir do ONTAP 9.15,1, os administradores podem configurar e ativar a autorização dinâmica no `visibility` modo para testar a configuração, ou no `enforced` modo para ativar a configuração para os usuários CLI que se conetam por SSH. Se você não precisar mais de autorização dinâmica, você pode desativá-la. Quando você desativa a autorização dinâmica, as configurações permanecem disponíveis e você pode usá-las mais tarde se decidir reativá-las.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-modify.html[`security dynamic-authorization modify` em referência de comando ONTAP.

Ativar autorização dinâmica para testes

Você pode ativar a autorização dinâmica no modo de visibilidade, que permite testar o recurso e garantir que os usuários não serão bloqueados acidentalmente. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas, mas não aplicada. No entanto, qualquer atividade que tenha sido negada ou

sujeita a desafios de autenticação adicionais é registrada. Como prática recomendada, você deve testar as configurações pretendidas neste modo antes de aplicá-las.

> Pode seguir este passo para ativar a autorização dinâmica pela primeira vez, mesmo que ainda não tenha configurado quaisquer outras definições de autorização dinâmica. "Personalizar autorização dinâmica"Consulte para obter instruções sobre como configurar outras definições de autorização dinâmica para personalizá-las para o seu ambiente.

Passos

1. Ative a autorização dinâmica no modo de visibilidade configurando as configurações globais e alterando o estado da função para `visibility`. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Parâmetros em negrito são necessários:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Verifique o resultado usando o `show` comando para exibir a configuração global:

```
security dynamic-authorization show
```

Ativar autorização dinâmica no modo imposto

Pode ativar a autorização dinâmica no modo imposto. Normalmente, você usa este modo depois de concluir o teste com o modo de visibilidade. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas e as restrições de atividade são aplicadas se as condições de restrição forem cumpridas. O intervalo de supressão também é aplicado, impedindo desafios de autenticação adicionais dentro do intervalo especificado.

> Esta etapa pressupõe que você configurou e ativou previamente a autorização dinâmica no `visibility` modo, o que é altamente recomendado.

Passos

1. Ative a autorização dinâmica no `enforced` modo alterando seu estado para `enforced`. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Parâmetros em negrito são necessários:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Verifique o resultado usando o `show` comando para exibir a configuração global:

```
security dynamic-authorization show
```

Desativar autorização dinâmica

Você pode desativar a autorização dinâmica se não precisar mais da segurança de autenticação adicionada.

Passos

1. Desative a autorização dinâmica alterando seu estado para `disabled`. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Parâmetros em negrito são necessários:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Verifique o resultado usando o `show` comando para exibir a configuração global:

```
security dynamic-authorization show
```

O que vem a seguir

(Opcional) dependendo do seu ambiente, "Personalizar autorização dinâmica"consulte para configurar outras definições de autorização dinâmica.

Personalizar autorização dinâmica no ONTAP

Como administrador, você pode personalizar diferentes aspetos de sua configuração de autorização dinâmica para aumentar a segurança das conexões SSH do administrador remoto ao cluster do ONTAP.

Pode personalizar as seguintes definições de autorização dinâmica, dependendo das suas necessidades de segurança:

- Configure as definições globais de autorização dinâmica
- Configurar componentes de pontuação de confiança de autorização dinâmica
- Configure um provedor de pontuação de confiança personalizado
- Configurar comandos restritos
- Configurar grupos de autorização dinâmicos

Configure as definições globais de autorização dinâmica

Você pode configurar configurações globais para autorização dinâmica, incluindo a VM de armazenamento para proteger, o intervalo de supressão para desafios de autenticação e as configurações de pontuação de

confiança.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-modify.html[`security dynamic-authorization modify` em referência de comando ONTAP.

Passos

1. Configurar definições globais para autorização dinâmica. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Veja a configuração resultante:

```
security dynamic-authorization show
```

Configurar comandos restritos

Quando você ativa a autorização dinâmica, o recurso inclui um conjunto padrão de comandos restritos. Você pode modificar esta lista para atender às suas necessidades. Consulte a "Documentação de verificação multi-admin (MAV)"para obter informações sobre a lista padrão de comandos restritos.

Adicionar um comando restrito

Você pode adicionar um comando à lista de comandos restritos com autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-rule-create.html[`security dynamic-authorization rule create` em referência de comando ONTAP.

Passos

1. Adicione o comando. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Veja a lista resultante de comandos restritos:

```
security dynamic-authorization rule show
```

Remover um comando restrito

Você pode remover um comando da lista de comandos que são restritos com autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-rule-delete.html[`security dynamic-authorization rule delete` em referência de comando ONTAP.

Passos

1. Remova o comando. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. Veja a lista resultante de comandos restritos:

```
security dynamic-authorization rule show
```

Configurar grupos de autorização dinâmicos

Por padrão, a autorização dinâmica se aplica a todos os usuários e grupos assim que você a ativar. No entanto, você pode criar grupos usando o `security dynamic-authorization group create` comando, para que a autorização dinâmica se aplique apenas a esses usuários específicos.

Adicione um grupo de autorização dinâmica

Pode adicionar um grupo de autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-group-create.html[`security dynamic-authorization group create` em referência de comando ONTAP.

Passos

1. Crie o grupo. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. Veja os grupos de autorização dinâmica resultantes:

```
security dynamic-authorization group show
```

Remova um grupo de autorização dinâmica

Pode remover um grupo de autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-group-delete.html[`security dynamic-authorization group delete` em referência de comando ONTAP.

Passos

1. Exclua o grupo. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Veja os grupos de autorização dinâmica resultantes:

```
security dynamic-authorization group show
```

Configurar componentes de pontuação de confiança de autorização dinâmica

Pode configurar o peso máximo da pontuação para alterar a prioridade dos critérios de pontuação ou remover determinados critérios da pontuação de risco.

Como uma prática recomendada, você deve deixar os valores de peso de pontuação padrão no lugar, e apenas ajustá-los se necessário.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-trust-score-component-modify.html[`security dynamic-authorization trust-score-component modify` em referência de comando ONTAP.

A seguir estão os componentes que você pode modificar, juntamente com sua pontuação padrão e pesos percentuais:

Critérios	Nome do componente	Peso bruto padrão da pontuação	Peso percentual padrão
Dispositivo confiável	`trusted-device`	20	50
Histórico de autenticação de login do usuário	`authentication-history`	20	50

Passos

1. Modificar componentes da pontuação de confiança. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Veja as configurações de componente de pontuação de confiança resultantes:

```
security dynamic-authorization trust-score-component show
```

Redefina a pontuação de confiança de um utilizador

Se um usuário tiver acesso negado devido a políticas do sistema e puder provar sua identidade, o administrador poderá redefinir a pontuação de confiança do usuário.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-Dynamic-Authorization-user-trust-reset.html'[`security dynamic-authorization user-trust-score reset` na referência de comando ONTAP.

Passos

1. Adicione o comando. Consulte a Configurar componentes de pontuação de confiança de autorização dinâmica para obter uma lista de componentes de pontuação de confiança que pode repor. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Exiba sua pontuação de confiança

Um usuário pode exibir sua própria pontuação de confiança para uma sessão de login.

Passos

1. Exiba sua pontuação de confiança:

```
security login whoami
```

Você deve ver saída semelhante ao seguinte:

```
User: admin
Role: admin
Trust Score: 50
```

Configure um provedor de pontuação de confiança personalizado

Se já receber métodos de pontuação de um fornecedor externo de pontuação de confiança, pode adicionar o fornecedor personalizado à configuração de autorização dinâmica.

Antes de começar

- O provedor de pontuação de confiança personalizado deve retornar uma resposta JSON. Os seguintes requisitos de sintaxe devem ser atendidos:
  - O campo que retorna a pontuação de confiança deve ser um campo escalar e não um elemento de um array.
  - O campo que retorna a pontuação de confiança pode ser um campo aninhado, `trust_score.value` como .
  - Deve haver um campo dentro da resposta JSON que retorna uma pontuação de confiança numérica. Se isso não estiver disponível nativamente, você pode escrever um script wrapper para retornar esse valor.
- O valor fornecido pode ser uma pontuação de confiança ou uma pontuação de risco. A diferença é que a pontuação de confiança está em ordem crescente com uma pontuação mais alta denotando um nível de confiança mais alto, enquanto a pontuação de risco está em ordem decrescente. Por exemplo, uma pontuação de confiança de 90 para uma faixa de pontuação de 0 a 100 indica que a pontuação é muito confiável e provavelmente resultará em uma "permissão" sem desafio adicional, enquanto uma pontuação de risco de 90 para uma faixa de pontuação de 0 a 100 indica alto risco e provavelmente resultará em uma "negação" sem um desafio adicional.
- O provedor de pontuação de confiança personalizado deve estar acessível por meio da API REST do ONTAP.
- O provedor de pontuação de confiança personalizado deve ser configurável usando um dos parâmetros suportados. Os provedores de pontuação de confiança personalizados que exigem configuração que não esteja na lista de parâmetros suportados não são suportados.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-trust-score-component-create.html[`security dynamic-authorization trust-score-component create` em referência de comando ONTAP.

Passos

1. Adicione um provedor de pontuação de confiança personalizado. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Veja as configurações do provedor de pontuação de confiança resultantes:

```
security dynamic-authorization trust-score-component show
```

Configurar etiquetas de fornecedor de pontuação de confiança personalizadas

Você pode se comunicar com provedores externos de pontuação de confiança usando tags. Isso permite que você envie informações no URL para o provedor de pontuação de confiança sem expor informações confidenciais.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-trust-score-component-create.html[`security dynamic-authorization trust-score-component create` em referência de comando ONTAP.

Passos

1. Ativar etiquetas de fornecedor de pontuação de confiança. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

   Por exemplo:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Autenticação e autorização usando OAuth 2,0

Visão geral da implementação do ONTAP OAuth 2,0

A partir do ONTAP 9.14, você tem a opção de controlar o acesso aos clusters do ONTAP usando a estrutura autorização aberta (OAuth 2,0). Você pode configurar esse recurso usando qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI do ONTAP, o Gerenciador do sistema e a API REST. No entanto, as decisões de autorização e controle de acesso do OAuth 2,0 só podem ser aplicadas quando um cliente acessa o ONTAP usando a API REST.

O suporte do OAuth 2,0 foi introduzido pela primeira vez com o ONTAP 9.14,0 e, portanto, sua disponibilidade depende da versão do ONTAP que você está usando. Consulte "Notas de versão do ONTAP" para obter mais informações.

Caraterísticas e benefícios

Os principais recursos e benefícios do uso do OAuth 2,0 com ONTAP são descritos abaixo.

Suporte para o padrão OAuth 2,0

OAuth 2,0 é o quadro de autorização padrão da indústria. Ele é usado para restringir e controlar o acesso a recursos protegidos usando tokens de acesso assinados. Existem vários benefícios para usar o OAuth 2,0:

- Muitas opções para a configuração de autorização
- Nunca revele as credenciais do cliente, incluindo senhas
- Os tokens podem ser definidos para expirar com base na sua configuração
- Ideal para uso com APIS REST

Testado com servidores de autorização populares

A implementação do ONTAP OAuth 2,0 foi testada com vários servidores ou serviços populares baseados na versão do ONTAP da seguinte forma:

- ONTAP 9.16,1 (suporte para UUUID do grupo para nomear o mapeamento e funções externas):
  - ID do Microsoft Entra
- ONTAP 9.14,1 (suporte para recursos padrão OAuth 2,0)
  - Auth0
  - Serviço de Federação do ative Directory (ADFS)
  - Capa da chave

"Servidores de autorização e tokens de acesso"Consulte para obter mais detalhes sobre os recursos e

recursos disponíveis em cada versão do ONTAP.

Suporte para vários servidores de autorização simultâneos

Você pode definir até oito servidores de autorização para um único cluster ONTAP. Isso oferece a flexibilidade para atender às necessidades de seu ambiente de segurança diversificado.

Integração com as funções REST

As decisões de autorização do ONTAP baseiam-se, em última análise, nas funções REST atribuídas a usuários ou grupos. Essas funções são realizadas no token de acesso como escopos autônomos ou baseadas em definições locais do ONTAP junto com grupos do ative Directory ou LDAP.

Opção para usar tokens de acesso com restrição de remetente

Você pode configurar o ONTAP e os servidores de autorização para usar a segurança de camada de transporte mútuo (MTLS), o que fortalece a autenticação do cliente. Ele garante que os tokens de acesso OAuth 2,0 são usados apenas pelos clientes para os quais foram emitidos originalmente. Esse recurso suporta e se alinha com várias recomendações de segurança populares, incluindo aquelas estabelecidas pela FAPI e MITER.

Implementação e configuração

Em um alto nível, há vários aspetos de uma implementação e configuração do OAuth 2,0 que você deve considerar ao começar.

OAuth 2,0 entidades dentro do ONTAP

A estrutura de autorização do OAuth 2,0 define várias entidades que podem ser mapeadas para elementos reais ou virtuais em seu data center ou rede. As entidades OAuth 2,0 e sua adaptação ao ONTAP são apresentadas na tabela abaixo.

Entidade OAuth 2,0	Descrição
Recurso	Os pontos de extremidade da API REST que fornecem acesso aos recursos do ONTAP por meio de comandos internos do ONTAP.
Proprietário do recurso	O usuário do cluster do ONTAP que criou o recurso protegido ou o possui por padrão.
Servidor de recursos	O host dos recursos protegidos que é o cluster do ONTAP.
Cliente	Um aplicativo solicitando acesso a um endpoint de API REST em nome ou com permissão do proprietário do recurso.
Servidor de autorização	Normalmente, um servidor dedicado responsável pela emissão de tokens de acesso e pela aplicação da política administrativa.

Configuração do Core ONTAP

Você precisa configurar o cluster ONTAP para ativar e usar o OAuth 2,0. Isso inclui estabelecer uma conexão com o servidor de autorização e definir a configuração de autorização ONTAP necessária. Você pode executar essa configuração usando qualquer uma das interfaces administrativas, incluindo:

- Interface de linha de comando ONTAP
- System Manager
- API REST do ONTAP

Ambiente e serviços de apoio

Além das definições do ONTAP, você também precisa configurar os servidores de autorização. Se você estiver usando o mapeamento grupo para função, também será necessário configurar os grupos do ative Directory ou o equivalente LDAP.

Clientes ONTAP suportados

A partir do ONTAP 9.14, um cliente API REST pode acessar o ONTAP usando o OAuth 2,0. Antes de emitir uma chamada de API REST, você precisa obter um token de acesso do servidor de autorização. Em seguida, o cliente passa esse token para o cluster ONTAP como um token *portador* usando o cabeçalho de solicitação de autorização HTTP. Dependendo do nível de segurança necessário, você também pode criar e instalar um certificado no cliente para usar tokens com restrição de remetente baseados no MTLS.

Terminologia selecionada

À medida que você começa a explorar uma implantação do OAuth 2,0 com o ONTAP, é útil se familiarizar com alguma terminologia. "Recursos adicionais"Consulte para obter links para mais informações sobre o OAuth 2,0.

Token de acesso

Um token emitido por um servidor de autorização e usado por um aplicativo cliente OAuth 2,0 para fazer solicitações para acessar os recursos protegidos.

JSON Web Token

O padrão usado para formatar os tokens de acesso. JSON é usado para representar as reivindicações OAuth 2,0 em um formato compacto com as reivindicações organizadas em três seções principais.

Token de acesso restrito ao remetente

Um recurso opcional baseado no protocolo MTLS (Mutual Transport Layer Security). Ao usar uma reivindicação de confirmação adicional no token, isso garante que o token de acesso seja usado apenas pelo cliente para o qual foi emitido originalmente.

Conjunto de chaves Web JSON

Um JWKS é uma coleção de chaves públicas usadas pelo ONTAP para verificar os tokens JWT apresentados pelos clientes. Os conjuntos de chaves estão normalmente disponíveis no servidor de autorização através de um URI dedicado.

Âmbito de aplicação

Os escopos fornecem uma maneira de limitar ou controlar o acesso de um aplicativo a recursos protegidos, como a API REST do ONTAP. Eles são representados como strings no token de acesso.

Função REST do ONTAP

As funções REST foram introduzidas com o ONTAP 9.6 e são uma parte essencial da estrutura RBAC do ONTAP. Essas funções são diferentes das funções tradicionais anteriores que ainda são suportadas pelo ONTAP. A implementação do OAuth 2,0 no ONTAP suporta apenas funções REST.

Cabeçalho de autorização HTTP

Um cabeçalho incluído na solicitação HTTP para identificar o cliente e as permissões associadas como parte de fazer uma chamada de API REST. Existem vários tipos ou implementações disponíveis dependendo de como a autenticação e a autorização são executadas. Ao apresentar um token de acesso OAuth 2,0 ao ONTAP, o token é identificado como um *token de portador*.

Autenticação básica HTTP

Uma técnica de autenticação HTTP inicial ainda suportada pelo ONTAP. As credenciais de texto simples (nome de usuário e senha) são concatenadas com dois pontos e codificadas em base64. A cadeia de

carateres é colocada no cabeçalho da solicitação de autorização e enviada para o servidor.

FAPI

Um grupo de trabalho da OpenID Foundation que fornece protocolos, esquemas de dados e recomendações de segurança para o setor financeiro. A API era originalmente conhecida como API Financial Grade.

MITRE

Uma empresa privada sem fins lucrativos que fornece orientação técnica e de segurança à força Aérea dos Estados Unidos e ao governo dos EUA.

Recursos adicionais

Vários recursos adicionais são fornecidos abaixo. Você deve revisar esses sites para obter mais informações sobre o OAuth 2,0 e os padrões relacionados.

Protocolos e padrões

- "RFC 6749: O OAuth 2,0 Authorization Framework"
- "RFC 7519: JSON Web tokens (JWT)"
- "RFC 7523: Perfil JSON Web Token (JWT) para permissões e autenticação de clientes OAuth 2,0"
- "RFC 7662: Introspeção de tokens OAuth 2,0"
- "RFC 7800: Chave de prova de posse para JWTs"
- "RFC 8705: Autenticação de cliente TLS mútuo OAuth 2,0 e tokens de acesso com certificado"

Organizações

- "Fundação OpenID"
- "Grupo de trabalho FAPI"
- "MITRE"
- "IANA - JWT"

Produtos e serviços

- "Auth0"
- "ID entra"
- "Visão geral da ADFS"
- "Capa da chave"

Ferramentas e utilitários adicionais

- "JWT por Auth0"
- "OpenSSL"

Documentação e recursos do NetApp

- "Documentação de automação do ONTAP"

Conceitos

Servidores de autorização e tokens de acesso

Os servidores de autorização executam várias funções importantes como um componente central dentro da estrutura de autorização do OAuth 2,0.

Servidores de autorização OAuth 2,0

Os servidores de autorização são os principais responsáveis pela criação e assinatura de tokens de acesso. Esses tokens contêm informações de identidade e autorização, permitindo que um aplicativo cliente acesse seletivamente recursos protegidos. Os servidores geralmente são isolados uns dos outros e podem ser implementados de várias maneiras diferentes, incluindo como um servidor dedicado autônomo ou como parte de um produto maior de gerenciamento de identidade e acesso.

> Terminologia diferente às vezes pode ser usada para um servidor de autorização, especialmente quando a funcionalidade OAuth 2,0 é empacotada dentro de um produto ou solução de gerenciamento de identidade e acesso maior. Por exemplo, o termo **provedor de identidade (IDP)** é frequentemente usado de forma intercambiável com **servidor de autorização**.

Administração

Além de emitir tokens de acesso, os servidores de autorização também fornecem serviços administrativos relacionados, normalmente através de uma interface de usuário da Web. Por exemplo, você pode definir e administrar:

- Autenticação de usuários e usuários
- Escopos
- Segregação administrativa através de inquilinos e reinos
- Aplicação da política
- Conexão com vários serviços externos
- Suporte para outros protocolos de identidade (como SAML)

O ONTAP é compatível com servidores de autorização compatíveis com o padrão OAuth 2,0.

Definindo para ONTAP

Você precisa definir um ou mais servidores de autorização para o ONTAP. O ONTAP se comunica com segurança com cada servidor para verificar tokens e executar outras tarefas relacionadas no suporte aos aplicativos cliente.

Os principais aspetos da configuração do ONTAP são apresentados abaixo. Consulte também "Cenários de implantação do OAuth 2,0"para obter mais informações.

Como e onde os tokens de acesso são validados

Existem duas opções para validar tokens de acesso.

- Validação local

  O ONTAP pode validar tokens de acesso localmente com base nas informações fornecidas pelo servidor de autorização que emitiu o token. As informações recuperadas do servidor de autorização são armazenadas em cache pelo ONTAP e atualizadas em intervalos regulares.

- Introspeção remota

  Você também pode usar introspeção remota para validar tokens no servidor de autorização. Introspeção é um protocolo que permite que partes autorizadas consultem um servidor de autorização sobre um token de acesso. Ele fornece ao ONTAP uma maneira de extrair determinados metadados de um token de acesso e validar o token. O ONTAP armazena em cache alguns dos dados por motivos de desempenho.

Localização da rede

O ONTAP pode estar atrás de um firewall. Nesse caso, você precisa identificar um proxy como parte da configuração.

Como os servidores de autorização são definidos

Você pode definir um servidor de autorização para o ONTAP usando qualquer uma das interfaces administrativas, incluindo a CLI, o Gerenciador de sistema ou a API REST. Por exemplo, com a CLI você usa o comando `security oauth2 client create`.

Número de servidores de autorização

Você pode definir até oito servidores de autorização para um único cluster ONTAP. O mesmo servidor de autorização pode ser definido mais de uma vez para o mesmo cluster do ONTAP desde que as reivindicações do emissor ou do emissor/público sejam únicas. Por exemplo, com KeyCloak, esse será sempre o caso ao usar reinos diferentes.

Recursos do OAuth 2,0 suportados no ONTAP

O suporte para OAuth 2,0 estava inicialmente disponível com o ONTAP 9.14,1 e continua sendo aprimorado com versões subsequentes. Os recursos do OAuth 2,0 suportados pelo ONTAP são descritos abaixo.

> Os recursos introduzidos com uma versão específica do ONTAP são levados para versões futuras.

ONTAP 9.16,1

O ONTAP 9.16,1 expande os recursos padrão do OAuth 2,0 para incluir extensões específicas do Entra ID para grupos nativos de ID do Entra. Isso envolve o uso de GUIDs no token de acesso em vez de nomes. Além disso, a versão adiciona suporte para mapeamento de funções externas para mapear as funções nativas do provedor de identidade para as funções do ONTAP usando o campo "funções" no token de acesso.

ONTAP 9.14,1

A partir do ONTAP 9.14,1, os servidores de autorização são suportados através dos seguintes recursos padrão do OAuth 2,0 para aplicativos que usam:

- OAuth 2,0 com os campos padrão, incluindo "iss", "AUD" e "exp", conforme descrito em "RFC6749: O Quadro de autorização OAuth 2,0" e "RFC 7519: JSON Web Token (JWT)". Isso também inclui suporte para identificar exclusivamente usuários através de campos no token de acesso, como "upn", "appid", "sub", "username" ou "Preferred_username".
- Extensões específicas do fornecedor ADFS para nomes de grupos com o campo "grupo".
- Extensões específicas do fornecedor do Azure para UUIDs de grupo com o campo "grupo".
- Extensões ONTAP para suporte de autorização usando funções independentes e nomeadas dentro do escopo do token de acesso OAuth 2,0. Isso inclui os campos "Escopo" e "scp", bem como os nomes de grupos dentro do escopo.

Usando tokens de acesso OAuth 2,0

Os tokens de acesso OAuth 2,0 emitidos pelos servidores de autorização são verificados pelo ONTAP e usados para tomar decisões de acesso baseadas em função para as solicitações de cliente de API REST.

Adquirir um token de acesso

Você precisa adquirir um token de acesso a partir de um servidor de autorização definido para o cluster ONTAP onde você usa a API REST. Para adquirir um token, você deve entrar em Contato diretamente com o servidor de autorização.

O ONTAP não emite tokens de acesso nem redireciona solicitações de clientes para os servidores de autorização.

A forma como você solicita um token depende de vários fatores, incluindo:

- Servidor de autorização e suas opções de configuração
- OAuth 2,0 tipo de concessão
- Ferramenta cliente ou software usada para emitir a solicitação

Tipos de concessão

Um *Grant* é um processo bem definido, incluindo um conjunto de fluxos de rede, usado para solicitar e receber um token de acesso OAuth 2,0. Vários tipos de concessão diferentes podem ser usados dependendo dos requisitos de cliente, ambiente e segurança. Uma lista dos tipos de concessão populares é apresentada na tabela abaixo.

Tipo de concessão	Descrição
Credenciais do cliente	Um tipo de concessão popular baseado no uso apenas de credenciais (como um ID e segredo compartilhado). Presume-se que o cliente tenha uma relação de confiança próxima com o proprietário do recurso.
Palavra-passe	O tipo de concessão de credenciais de senha do proprietário do recurso pode ser usado nos casos em que o proprietário do recurso tenha uma relação de confiança estabelecida com o cliente. Também pode ser útil ao migrar clientes HTTP legados para o OAuth 2,0.
Código de autorização	Este é um tipo de concessão ideal para clientes confidenciais e é baseado em um fluxo baseado em redirecionamento. Ele pode ser usado para obter um token de acesso e atualizar token.

Conteúdo do JWT

Um token de acesso OAuth 2,0 é formatado como JWT. O conteúdo é criado pelo servidor de autorização com base na sua configuração. No entanto, os tokens são opacos para as aplicações cliente. Um cliente não tem razão para inspecionar um token ou estar ciente do conteúdo.

Cada token de acesso JWT contém um conjunto de reivindicações. As reclamações descrevem as caraterísticas do emissor e a autorização com base nas definições administrativas do servidor de autorização. Algumas das reclamações registadas com a norma estão descritas na tabela abaixo. Todas as cordas são sensíveis a maiúsculas e minúsculas.

Pedido de reembolso	Palavra-chave	Descrição
Emissor	iss	Identifica o principal que emitiu o token. O processamento da reclamação é específico da aplicação.
Assunto	sub	O assunto ou usuário do token. O nome é definido para ser global ou localmente único.
Público-alvo	aud	Os destinatários para os quais o token se destina. Implementado como uma matriz de strings.
Expiração	exp	O tempo após o qual o token expira e deve ser rejeitado.

Consulte "RFC 7519: JSON Web tokens" para obter mais informações.

Autorização do cliente

Visão geral e opções para autorização de cliente ONTAP

A implementação do ONTAP OAuth 2,0 foi projetada para ser flexível e robusta, fornecendo os recursos necessários para proteger seu ambiente ONTAP. Existem várias opções de configuração mutuamente exclusivas disponíveis. As decisões de autorização são, em última análise, baseadas nas funções REST do ONTAP contidas ou derivadas dos tokens de acesso OAuth 2,0.

Você só pode usar "Funções REST do ONTAP" ao configurar a autorização para o OAuth 2,0. As funções tradicionais anteriores do ONTAP não são suportadas.

O ONTAP aplica a única opção de autorização mais adequada com base na sua configuração. "Como o ONTAP determina o acesso"Consulte para obter mais informações sobre como o ONTAP toma decisões de acesso ao cliente.

Escopos auto-contidos OAuth 2,0

Esses escopos contêm uma ou mais funções REST personalizadas, cada uma encapsulada em uma única cadeia no token de acesso. Eles são independentes das definições de função do ONTAP. Você precisa configurar as strings de escopo em seu servidor de autorização. Consulte "Escopos OAuth 2,0 independentes" para obter mais informações.

Funções REST do ONTAP local

Uma única função REST nomeada, seja builtin ou personalizado, pode ser usada. A sintaxe do escopo para uma função nomeada é **ONTAP-role-** com codificação URL-ONTAP-role-name>. Por exemplo, se a função ONTAP for `admin` a string Escopo será `ontap-role-admin`.

Usuários

O nome de usuário no token de acesso definido com acesso ao aplicativo "http" pode ser usado. Um usuário é testado na seguinte ordem com base no método de autenticação definido: Senha, domínio (ative Directory), nsswitch (LDAP).

Grupos

Os servidores de autorização podem ser configurados para usar grupos ONTAP para autorização. Se as definições locais do ONTAP forem examinadas, mas não for possível tomar nenhuma decisão de acesso, os grupos do ative Directory ("domínio") ou LDAP ("nsswitch") serão usados. As informações do grupo podem ser

especificadas de duas maneiras:

- OAuth 2,0 string de escopo

  Suporta aplicativos confidenciais usando o fluxo de credenciais de cliente onde não há usuário com uma associação de grupo. O escopo deve ser nomeado **ONTAP-group-** com codificação URL-ONTAP-group-name>. Por exemplo, se o grupo for "desenvolvimento", a string de escopo será "ONTAP-group-development".

- Na reclamação "Group" (grupo)

  Isso é destinado a tokens de acesso emitidos pelo ADFS usando o fluxo proprietário do recurso (concessão de senha).

Consulte "Trabalhar com grupos" para obter mais informações.

Escopos OAuth 2,0 independentes

Escopos auto-contidos são strings transportadas no token de acesso. Cada uma é uma definição completa de função personalizada e inclui tudo o que a ONTAP precisa para tomar uma decisão de acesso. O escopo é separado e distinto de qualquer uma das funções REST definidas no próprio ONTAP.

Formato da cadeia de escopo

Em um nível base, o escopo é representado como uma cadeia contígua e composto por seis valores separados por dois pontos. Os parâmetros usados na cadeia de escopo são descritos abaixo.

ONTAP literal

O escopo deve começar com o valor literal `ontap` em minúsculas. Isso identifica o escopo como específico do ONTAP.

Cluster

Isso define a que cluster ONTAP o escopo se aplica. Os valores podem incluir:

- UUID do cluster

  Identifica um único cluster.

- Asterisco (*)

  Indica que o escopo se aplica a todos os clusters.

Você pode usar o comando ONTAP CLI `cluster identity show` para exibir o UUID do cluster. Se não for especificado, o escopo se aplica a todos os clusters.

Função

O nome do papel RESTANTE contido no escopo auto-contido. Esse valor não é examinado pelo ONTAP nem correspondido a nenhuma função REST existente definida como ONTAP. O nome é utilizado para registar.

Nível de acesso

Esse valor indica o nível de acesso aplicado ao aplicativo cliente ao usar o endpoint da API no escopo. Existem seis valores possíveis, conforme descrito na tabela abaixo.

Nível de acesso	Descrição
nenhum	Nega todo o acesso ao endpoint especificado.
readonly	Permite apenas acesso de leitura utilizando O GET.
read_create	Permite o acesso de leitura, bem como a criação de novas instâncias de recursos usando POST.
read_modify	Permite acesso de leitura, bem como a capacidade de atualizar os recursos existentes USANDO PATCH.
read_create_modify	Permite todo o acesso, exceto apagar. As operações permitidas incluem GET (read), POST (Create) e PATCH (update).
tudo	Permite acesso total.

SVM

O nome da SVM no cluster ao qual o escopo se aplica. Use o valor * (asterisco) para indicar todos os SVMs.

> Esta funcionalidade não é totalmente suportada com o ONTAP 9.14,1. Você pode ignorar o parâmetro SVM e usar um asterisco como um marcador de posição. Revise o "Notas de versão do ONTAP" para verificar se há suporte futuro à SVM.

URI DA API REST

O caminho completo ou parcial para um recurso ou conjunto de recursos relacionados. A string deve começar com `/api`. Se você não especificar um valor, o escopo se aplica a todos os endpoints da API no cluster do ONTAP.

Exemplos de escopo

Alguns exemplos de escopos auto-contidos são apresentados abaixo.

ONTAP:*:joes-role:read_create_modify:*:/api/cluster

Fornece ao usuário atribuído essa função de leitura, criação e modificação do acesso ao `/cluster` endpoint.

Ferramenta administrativa CLI

Para tornar a administração dos escopos auto-contidos mais fácil e menos propensa a erros, o ONTAP fornece o comando CLI `security oauth2 scope` para gerar strings de escopo com base em seus parâmetros de entrada.

O comando `security oauth2 scope` tem dois casos de uso com base na sua entrada:

- Parâmetros CLI para string de escopo

  Você pode usar esta versão do comando para gerar uma string de escopo com base nos parâmetros de entrada.

- String de escopo para parâmetros CLI

  Você pode usar esta versão do comando para gerar os parâmetros do comando com base na cadeia de carateres de escopo de entrada.

Exemplo

O exemplo a seguir gera uma string de escopo com a saída incluída após o exemplo de comando abaixo. A definição se aplica a todos os clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Trabalhar com grupos

O ONTAP fornece várias opções para configurar grupos com base no servidor de autorização. Os grupos podem então ser mapeados para funções que são usadas pelo ONTAP para determinar o acesso.

Como os grupos são identificados

Quando você configura um grupo em um servidor de autorização, ele é identificado e transportado em um token de acesso OAuth 2,0 usando um nome ou UUID. Você precisa estar ciente de como o servidor de autorização lida com grupos antes de configurar o ONTAP.

> Se vários grupos forem incluídos em um token de acesso, o ONTAP tentará usar cada um até que haja uma correspondência.

Nomes de grupos

Muitos servidores de autorização identificam e representam grupos usando um nome. Aqui está um fragmento de um token de acesso JSON gerado pelo Serviço de Federação do ative Directory (ADFS) contendo vários grupos. Consulte Gerenciar grupos com nomes para obter mais informações.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUUIDs de grupo

Alguns servidores de autorização identificam e representam grupos usando um UUID. Aqui está um fragmento de um token de acesso JSON gerado pelo Microsoft Entra ID contendo vários grupos. Consulte Gerenciar grupos com UUIDs para obter mais informações.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Gerenciar grupos com nomes

Se o servidor de autorização usar nomes para identificar grupos, você precisa garantir que cada grupo esteja definido como ONTAP. Dependendo do seu ambiente de segurança, talvez você já tenha o grupo definido.

Aqui está um exemplo de comando CLI definindo um grupo para ONTAP. Observe que está usando um grupo nomeado do token de acesso de amostra. Você precisa estar no nível de privilégio ONTAP **admin** para emitir o comando.

Exemplo

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Você também pode configurar esse recurso usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Gerenciar grupos com UUIDs

Se o servidor de autorização representar grupos usando valores UUID, você precisará executar uma configuração de duas etapas antes de usar um grupo. A partir do ONTAP 9.16,1, dois recursos de mapeamento estão disponíveis e foram testados com o Microsoft Entra ID. Você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos CLI.

Você também pode configurar esses recursos usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Informações relacionadas

- "Comandos CLI do ONTAP"

Mapear um UUID de grupo para um nome de grupo

Se você estiver usando um servidor de autorização que representa grupos usando valores UUID, será necessário mapear os UUIDs do grupo para nomes de grupos. As principais operações da CLI do ONTAP são

descritas abaixo.

Criar

Você pode definir uma nova configuração de mapeamento de grupo com o `security login group create` comando. O UUID e o nome do grupo devem corresponder à configuração no servidor de autorização.

Parâmetros

Os parâmetros usados para criar um mapeamento de grupo são descritos abaixo.

Parâmetro	Descrição
`vserver`	Opcionalmente, especifica o nome do SVM (vserver) ao qual o grupo está associado. Se omitido, o grupo está associado ao cluster ONTAP.
`name`	O nome exclusivo do grupo que o ONTAP usará.
`type`	Este valor indica o provedor de identidade do qual o grupo se origina.
`uuid`	Especifica o identificador universalmente exclusivo do grupo, conforme fornecido pelo servidor de autorização.

Aqui está um exemplo de comando CLI definindo um grupo para ONTAP. Observe que está usando um grupo UUID do token de acesso de amostra.

Exemplo

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Depois de criar o grupo, um identificador inteiro exclusivo somente leitura é gerado para o grupo.

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Você pode usar a `show` opção para recuperar o ID de grupo exclusivo gerado para um grupo. Consulte a documentação de referência dos comandos ONTAP para obter mais informações.

Mapear um UUID de grupo para uma função

Se você estiver usando um servidor de autorização que representa grupos usando valores UUID, você poderá mapear o grupo para uma função. As principais operações da CLI do ONTAP são descritas abaixo. Além disso, você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos.

> Você precisa primeiro Mapear um UUID de grupo para um nome de grupo e recuperar o ID inteiro exclusivo gerado para o grupo. Você precisará do ID para mapear o grupo para uma função.

Criar

Você pode definir um novo mapeamento de função com o `security login group role-mapping create` comando.

Parâmetros

Os parâmetros usados para mapear um grupo para uma função são descritos abaixo.

Parâmetro	Descrição
`group-id`	Especifica o ID exclusivo gerado para o grupo usando o comando `security login group create`.
`role`	O nome da função ONTAP para o qual o grupo é mapeado.

Exemplo

```
security login group role-mapping create -group-id 1 -role admin
```

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Consulte a documentação de referência dos comandos ONTAP para obter mais informações.

Mapeamento de funções externas

Uma função externa é definida em um provedor de identificação configurado para uso pelo ONTAP. Você pode criar e administrar relacionamentos de mapeamento entre essas funções externas e as funções do ONTAP usando a CLI do ONTAP.

Você também pode configurar o recurso de mapeamento de função externa usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Informações relacionadas

- "Comandos CLI do ONTAP".

Funções externas em um token de acesso

Aqui está um fragmento de um token de acesso JSON contendo dois papéis externos.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuração

Você pode usar a interface de linha de comando ONTAP para administrar o recurso de mapeamento de função externa.

Criar

Você pode definir uma configuração de mapeamento de função com o `security login external-role-mapping create` comando. Você precisa estar no nível de privilégio ONTAP **admin** para emitir este comando, bem como as opções relacionadas.

Parâmetros

Os parâmetros usados para criar um mapeamento de grupo são descritos abaixo.

Parâmetro	Descrição
`external-role`	O nome da função definida no provedor de identidade externo.
`provider`	O nome do provedor de identidade. Este deve ser o identificador do sistema.
`ontap-role`	Indica a função ONTAP existente para a qual a função externa está mapeada.

Exemplo

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Consulte a documentação de referência dos comandos do ONTAP ou as páginas man da CLI do ONTAP para obter mais informações.

Como o ONTAP determina o acesso do cliente

Para projetar e implementar adequadamente o OAuth 2,0, você precisa entender como sua configuração de autorização é usada pelo ONTAP para tomar decisões de acesso para os clientes. As principais etapas usadas para determinar o acesso são apresentadas abaixo com base na versão do ONTAP.

Não houve atualizações significativas do OAuth 2,0 com o ONTAP 9.15,1. Se estiver a utilizar a versão 9.15.1, consulte a descrição do ONTAP 9.14,1.

Informações relacionadas

- "Recursos do OAuth 2,0 suportados no ONTAP"

ONTAP 9.16,1

O ONTAP 9.16,1 expande o suporte padrão do OAuth 2,0 para incluir extensões específicas do Microsoft Entra ID para grupos nativos de ID do Entra, bem como mapeamento de funções externas.

Determine o acesso do cliente para o ONTAP 9.16,1

Passo 1: Escopos auto-contidos

Se o token de acesso contiver quaisquer escopos auto-contidos, o ONTAP examina esses escopos primeiro. Se não existirem escopos auto-suficientes, avance para o passo 2.

Com um ou mais escopos independentes presentes, o ONTAP aplica cada escopo até que uma decisão explícita de **PERMITIR** ou **NEGAR** possa ser tomada. Se uma decisão explícita for tomada, o processamento termina.

Se o ONTAP não conseguir tomar uma decisão de acesso explícito, avance para o passo 2.

Passo 2: Verifique o sinalizador de funções locais

ONTAP examina o parâmetro booleano `use-local-roles-if-present` . O valor deste sinalizador é definido separadamente para cada servidor de autorização definido como ONTAP.

- Se o valor for `true`, avance para o passo 3.
- Se o valor estiver `false` a processar termina e o acesso for negado.

Passo 3: Nomeado ONTAP REST role

Se o token de acesso contiver uma FUNÇÃO REST nomeada `scope` no campo ou `scp`, ou como uma reivindicação, o ONTAP usará a função para tomar a decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento termina.

Se não houver nenhuma função REST nomeada ou a função não for encontrada, continue para a etapa 4.

Passo 4: Usuários

Extraia o nome de usuário do token de acesso e tente combiná-lo com os usuários que têm acesso ao aplicativo "http". Os usuários são examinados com base no método de autenticação na seguinte ordem:

- palavra-passe
- Domínio (ative Directory)
- Nsswitch (LDAP)

Se um usuário correspondente for encontrado, o ONTAP usará a função definida para que o usuário tome uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se um usuário não for correspondido ou se não houver nome de usuário no token de acesso, continue para a etapa 5.

Passo 5: Grupos

Se um ou mais grupos forem incluídos, o formato será examinado. Se os grupos forem representados como UUIDs, uma tabela de mapeamento de grupo interno será pesquisada. Se houver uma correspondência de grupo e uma função associada, o ONTAP usará a função definida para o grupo tomar uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina. Para obter mais informações, "Trabalhar com grupos"consulte .

Se os grupos forem representados como nomes e configurados com autorização de domínio ou nsswitch, o ONTAP tentará combiná-los com um grupo do ative Directory ou LDAP, respetivamente. Se houver uma correspondência de grupo, o ONTAP usará a função definida para o grupo tomar uma

decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se não houver correspondência de grupo ou se não houver nenhum grupo no token de acesso, o acesso será negado e o processamento será concluído.

ONTAP 9.14,1

O OAuth 2,0 inicial suportado é introduzido com o ONTAP 9.14,1 com base nos recursos padrão do OAuth 2,0.

Determine o acesso do cliente para o ONTAP 9.14,1

Passo 1: Escopos auto-contidos

Se o token de acesso contiver quaisquer escopos auto-contidos, o ONTAP examina esses escopos primeiro. Se não existirem escopos auto-suficientes, avance para o passo 2.

Com um ou mais escopos independentes presentes, o ONTAP aplica cada escopo até que uma decisão explícita de **PERMITIR** ou **NEGAR** possa ser tomada. Se uma decisão explícita for tomada, o processamento termina.

Se o ONTAP não conseguir tomar uma decisão de acesso explícito, avance para o passo 2.

Passo 2: Verifique o sinalizador de funções locais

ONTAP examina o parâmetro booleano `use-local-roles-if-present` . O valor deste sinalizador é definido separadamente para cada servidor de autorização definido como ONTAP.

- Se o valor for `true`, avance para o passo 3.
- Se o valor estiver `false` a processar termina e o acesso for negado.

Passo 3: Nomeado ONTAP REST role

Se o token de acesso contiver uma FUNÇÃO REST nomeada `scope` no campo ou `scp`, o ONTAP usará a função para tomar a decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento termina.

Se não houver nenhuma função REST nomeada ou a função não for encontrada, continue para a etapa 4.

Passo 4: Usuários

Extraia o nome de usuário do token de acesso e tente combiná-lo com os usuários que têm acesso ao aplicativo "http". Os usuários são examinados com base no método de autenticação na seguinte ordem:

- palavra-passe
- Domínio (ative Directory)
- Nsswitch (LDAP)

Se um usuário correspondente for encontrado, o ONTAP usará a função definida para que o usuário tome uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se um usuário não for correspondido ou se não houver nome de usuário no token de acesso, continue para a etapa 5.

Passo 5: Grupos

Se um ou mais grupos forem incluídos e configurados com autorização de domínio ou nsswitch, o ONTAP tentará combiná-los com um grupo do ative Directory ou LDAP, respetivamente.

Se houver uma correspondência de grupo, o ONTAP usará a função definida para o grupo tomar uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se não houver correspondência de grupo ou se não houver nenhum grupo no token de acesso, o acesso será negado e o processamento será concluído.

Cenários de implantação do OAuth 2,0

Há várias opções de configuração disponíveis ao definir um servidor de autorização para o ONTAP. Com base nessas opções, você pode definir um servidor de autorização apropriado para o seu ambiente usando um dos vários cenários de implantação.

Resumo dos parâmetros de configuração

Existem vários parâmetros de configuração disponíveis ao definir um servidor de autorização para o ONTAP. Estes parâmetros são geralmente suportados em todas as interfaces administrativas.

> O nome usado para um parâmetro ou campo individual pode variar dependendo da interface administrativa do ONTAP. Para acomodar as diferenças nas interfaces administrativas, um único nome genérico é usado para cada parâmetro na tabela. O nome exato usado com uma interface específica deve ser óbvio com base no contexto.

Parâmetro	Descrição
Nome	O nome do servidor de autorização como é conhecido pelo ONTAP.
Aplicação	A aplicação interna do ONTAP à qual a definição se aplica. Este deve ser **http**.
URI do emissor	O FQDN com o caminho que identifica o site ou a organização que emite os tokens.
URI do provedor JWKS	O FQDN com caminho e nome de arquivo onde o ONTAP obtém os conjuntos de chaves da Web JSON usados para validar os tokens de acesso.
Intervalo de atualização do JWKS	O intervalo de tempo que determina com que frequência o ONTAP atualiza informações de certificado do URI JWKS do provedor. O valor é especificado no formato ISO-8601.
Endpoint de introspeção	O FQDN com caminho que o ONTAP usa para executar a validação remota de token por meio de introspeção.
ID do cliente	O nome do cliente, conforme definido no servidor de autorização. Quando esse valor é incluído, você também precisa fornecer o segredo do cliente associado com base na interface.
Proxy de saída	Isso é para fornecer acesso ao servidor de autorização quando o ONTAP está atrás de um firewall. O URI deve estar no formato curl.
Use funções locais, se presentes	Um sinalizador booleano que determina se as definições ONTAP locais são usadas, incluindo uma FUNÇÃO REST nomeada e usuários locais.
Reclamação do utilizador remoto	Um nome alternativo que o ONTAP usa para corresponder aos usuários locais. Use o `sub` campo no token de acesso para corresponder ao nome de usuário local.
Público-alvo	Este campo define os endpoints onde o token de acesso pode ser usado.

Cenários de implantação

Vários cenários comuns de implantação são apresentados abaixo. Eles são organizados com base se a validação de token é realizada localmente pelo ONTAP ou remotamente pelo servidor de autorização. Cada cenário inclui uma lista das opções de configuração necessárias. "Implantar o OAuth 2,0 no ONTAP"Consulte para obter exemplos dos comandos de configuração.

Depois de definir um servidor de autorização, você pode exibir sua configuração por meio da interface administrativa do ONTAP. Por exemplo, use o comando `security oauth2 client show` com a CLI do ONTAP.

Validação local

Os cenários de implantação a seguir são baseados no ONTAP executando a validação de token localmente.

Use escopos autônomos sem um proxy

Esta é a implantação mais simples usando apenas escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade ONTAP local é usada. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- URI do emissor

Você também precisa adicionar os escopos no servidor de autorização.

Use escopos autônomos com um proxy

Esse cenário de implantação usa os escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade ONTAP local é usada. Mas o servidor de autorização está atrás de um firewall e, portanto, você precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Proxy de saída
- URI do emissor
- Público-alvo

Você também precisa adicionar os escopos no servidor de autorização.

Use funções de usuário local e mapeamento de nome de usuário padrão com um proxy

Esse cenário de implantação usa funções de usuário local com mapeamento de nomes padrão. A reivindicação de usuário remoto usa o valor padrão de `sub` e, portanto, esse campo no token de acesso é usado para corresponder ao nome de usuário local. O nome de usuário deve ter 40 carateres ou menos. O servidor de autorização está atrás de um firewall, então você também precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Usar funções locais, se presentes (`true`)
- Proxy de saída
- Emissor

Tem de se certificar de que o utilizador local está definido como ONTAP.

Use funções de usuário local e mapeamento de nome de usuário alternativo com um proxy

Esse cenário de implantação usa funções de usuário local com um nome de usuário alternativo que é usado para corresponder a um usuário local do ONTAP. O servidor de autorização está atrás de um firewall, então você precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Usar funções locais, se presentes (`true`)
- Reclamação do utilizador remoto
- Proxy de saída
- URI do emissor
- Público-alvo

Tem de se certificar de que o utilizador local está definido como ONTAP.

Introspeção remota

As configurações de implantação a seguir são baseadas no ONTAP executando a validação de token remotamente por meio de introspeção.

Use escopos autônomos sem proxy

Esta é uma implantação simples baseada no uso dos escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade do ONTAP é usada. Você deve incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- Endpoint de introspeção
- ID do cliente
- URI do emissor

Você precisa definir os escopos, bem como o segredo do cliente e do cliente no servidor de autorização.

Autenticação de cliente usando TLS mútuo

Dependendo de suas necessidades de segurança, você pode configurar opcionalmente o TLS mútuo (MTLS) para implementar uma autenticação de cliente forte. Quando usado com o ONTAP como parte de uma implantação do OAuth 2,0, o MTLS garante que os tokens de acesso são usados apenas pelos clientes aos quais foram emitidos originalmente.

TLS mútuo com OAuth 2,0

O Transport Layer Security (TLS) é usado para estabelecer um canal de comunicação seguro entre dois aplicativos, normalmente um navegador cliente e um servidor da Web. O TLS mútuo estende isso fornecendo uma forte identificação do cliente através de um certificado de cliente. Quando usado em um cluster ONTAP

com OAuth 2,0, a funcionalidade base MTLS é estendida criando e usando tokens de acesso restritos ao remetente.

Um token de acesso restrito ao remetente só pode ser usado pelo cliente para o qual foi emitido originalmente. Para suportar esse recurso, uma nova solicitação de confirmação (`cnf`) é inserida no token. O campo contém uma propriedade `x5t#S256` que contém um resumo do certificado de cliente usado ao solicitar o token de acesso. Esse valor é verificado pela ONTAP como parte da validação do token. Os tokens de acesso emitidos por servidores de autorização que não estão restritos ao remetente não incluem a reivindicação de confirmação adicional.

Você precisa configurar o ONTAP para usar o MTLS separadamente para cada servidor de autorização. Por exemplo, o comando CLI `security oauth2 client` inclui o parâmetro `use-mutual-tls` para controlar o processamento MTLS com base em três valores, como mostrado na tabela abaixo.

Em cada configuração, o resultado e a ação tomadas pelo ONTAP dependem do valor do parâmetro de configuração, bem como do conteúdo do token de acesso e do certificado do cliente. Os parâmetros na tabela são organizados do mínimo ao mais restritivo.

Parâmetro	Descrição
nenhum	A autenticação TLS mútua OAuth 2,0 está completamente desativada para o servidor de autorização. A ONTAP não executará a autenticação de certificado de cliente MTLS, mesmo que a reclamação de confirmação esteja presente no token ou um certificado de cliente seja fornecido com a conexão TLS.
pedido	A autenticação TLS mútua do OAuth 2,0 é aplicada se um token de acesso restrito ao remetente for apresentado pelo cliente. Ou seja, o MTLS é aplicado somente se a reivindicação de confirmação (com propriedade `x5t#S256`) estiver presente no token de acesso. Esta é a configuração padrão.
obrigatório	A autenticação TLS mútua OAuth 2,0 é aplicada para todos os tokens de acesso emitidos pelo servidor de autorização. Portanto, todos os tokens de acesso devem ser restritos ao remetente. A autenticação e a solicitação de API REST falharão se a solicitação de confirmação não estiver presente no token de acesso ou se houver um certificado de cliente inválido.

Fluxo de implementação de alto nível

As etapas típicas envolvidas ao usar o MTLS com o OAuth 2,0 em um ambiente ONTAP são apresentadas abaixo. "RFC 8705: Autenticação de cliente TLS mútuo OAuth 2,0 e tokens de acesso com certificado"Consulte para obter mais detalhes.

Passo 1: Criar e instalar um certificado de cliente

O estabelecimento da identidade do cliente é baseado na comprovação do conhecimento de uma chave privada do cliente. A chave pública correspondente é colocada em um certificado X,509 assinado apresentado pelo cliente. Em alto nível, as etapas envolvidas na criação do certificado de cliente incluem:

1. Gere um par de chaves públicas e privadas
2. Crie uma solicitação de assinatura de certificado
3. Envie o arquivo CSR para uma CA conhecida
4. A CA verifica a solicitação e emite o certificado assinado

Normalmente, você pode instalar o certificado de cliente em seu sistema operacional local ou usá-lo

diretamente com um utilitário comum, como curl.

Passo 2: Configure o ONTAP para usar o MTLS

Você precisa configurar o ONTAP para usar o MTLS. Esta configuração é feita separadamente para cada servidor de autorização. Por exemplo, com a CLI o comando `security oauth2 client` é usado com o parâmetro opcional `use-mutual-tls` . Consulte "Implantar o OAuth 2,0 no ONTAP" para obter mais informações.

Passo 3: O cliente solicita um token de acesso

O cliente precisa solicitar um token de acesso do servidor de autorização configurado para ONTAP. O aplicativo cliente deve usar o MTLS com o certificado criado e instalado na etapa 1.

Passo 4: O servidor de autorização gera o token de acesso

O servidor de autorização verifica a solicitação do cliente e gera um token de acesso. Como parte disso, ele cria um resumo de mensagem do certificado do cliente que é incluído no token como uma reivindicação de confirmação (campo `cnf`).

Passo 5: O aplicativo cliente apresenta o token de acesso ao ONTAP

O aplicativo cliente faz uma chamada de API REST para o cluster ONTAP e inclui o token de acesso no cabeçalho da solicitação de autorização como um **token de portador**. O cliente deve usar o MTLS com o mesmo certificado usado para solicitar o token de acesso.

Passo 6: O ONTAP verifica o cliente e o token.

O ONTAP recebe o token de acesso em uma solicitação HTTP, bem como o certificado de cliente usado como parte do processamento do MTLS. O ONTAP primeiro valida a assinatura no token de acesso. Com base na configuração, o ONTAP gera um resumo de mensagem do certificado do cliente e compara-o com a reclamação de confirmação **cnf** no token. Se os dois valores corresponderem, o ONTAP confirmou que o cliente que faz a solicitação de API é o mesmo cliente para o qual o token de acesso foi originalmente emitido.

Configurar e implantar

Prepare-se para implantar o OAuth 2,0 com o ONTAP

Antes de configurar o OAuth 2,0 em um ambiente ONTAP, você deve se preparar para a implantação. Um resumo das principais tarefas e decisões está incluído abaixo. O arranjo das seções é geralmente alinhado com a ordem que você deve seguir. Mas, embora seja aplicável à maioria das implantações, você deve adaptá-lo ao seu ambiente conforme necessário. Você também deve considerar a criação de um plano de implantação formal.

Com base no seu ambiente, pode selecionar a configuração para os servidores de autorização definidos para o ONTAP. Isso inclui os valores de parâmetro que você precisa especificar para cada tipo de implantação. Consulte "Cenários de implantação do OAuth 2,0" para obter mais informações.

Recursos protegidos e aplicativos de clientes

O OAuth 2,0 é uma estrutura de autorização para controlar o acesso a recursos protegidos. Diante disso, um primeiro passo importante com qualquer implantação é determinar quais são os recursos disponíveis e quais clientes precisam acessar.

Identificar aplicativos clientes

Você precisa decidir quais clientes usarão o OAuth 2,0 ao emitir chamadas de API REST e quais endpoints de API eles precisam acessar.

Analise as funções REST do ONTAP e os usuários locais existentes

Você deve rever as definições de identidade do ONTAP existentes, incluindo as funções REST e os usuários locais. Dependendo de como você configura o OAuth 2,0, essas definições podem ser usadas para tomar decisões de acesso.

Transição global para o OAuth 2,0

Embora você possa implementar a autorização do OAuth 2,0 gradualmente, você também pode mover todos os clientes de API REST para o OAuth 2,0 imediatamente definindo um sinalizador global para cada servidor de autorização. Isso permite que as decisões de acesso sejam tomadas com base na configuração existente do ONTAP sem a necessidade de criar escopos autônomos.

Servidores de autorização

Os servidores de autorização desempenham um papel importante na implantação do OAuth 2,0, emitindo tokens de acesso e impondo a política administrativa.

Selecione e instale o servidor de autorização

Você precisa selecionar e instalar um ou mais servidores de autorização. É importante familiarizar-se com as opções de configuração e procedimentos dos seus provedores de identidade, incluindo como definir escopos. Observe que alguns servidores de autorização, incluindo o Microsoft Entra ID, representam grupos usando UUIDs em vez de nomes.

Determine se o certificado de CA raiz de autorização precisa ser instalado

O ONTAP usa o certificado do servidor de autorização para validar os tokens de acesso assinados apresentados pelos clientes. Para fazer isso, o ONTAP precisa do certificado de CA raiz e de quaisquer certificados intermediários. Estes podem ser pré-instalados com o ONTAP. Se não, você precisa instalá-los.

Avaliar a localização e a configuração da rede

Se o servidor de autorização estiver atrás de um firewall, o ONTAP precisa ser configurado para usar um servidor proxy.

Autenticação e autorização do cliente

Existem vários aspetos da autenticação e autorização do cliente que você precisa considerar.

Escopos auto-contidos ou definições de identidade ONTAP local

Em um alto nível, você pode definir escopos autônomos definidos no servidor de autorização ou confiar nas definições de identidade ONTAP locais existentes, incluindo funções e usuários.

Opções com processamento ONTAP local

Se você usar as definições de identidade do ONTAP, você deve decidir qual aplicar, incluindo:

- Função REST nomeada
- Corresponder a utilizadores locais
- Grupos do ative Directory ou LDAP

Validação local ou introspeção remota

Você precisa decidir se os tokens de acesso serão validados localmente pelo ONTAP ou no servidor de

autorização por meio de introspeção. Há também vários valores relacionados a serem considerados, como o intervalo de atualização.

Tokens de acesso restrito ao remetente

Para ambientes que exigem um alto nível de segurança, você pode usar tokens de acesso com restrição de envio baseados em MTLS. Isso requer um certificado para cada cliente.

Grupos como UUIDs e mapeamento de identidade

Se você estiver usando um servidor de autorização que representa grupos usando UUIDs, você precisará Planejar como mapeá-los para nomes de grupos e, possivelmente, para funções associadas.

Interface administrativa

Você pode executar a administração do OAuth 2,0 por meio de qualquer uma das interfaces do ONTAP, incluindo:

- Interface de linha de comando
- System Manager
- API REST

Como os clientes solicitam tokens de acesso

Os aplicativos cliente devem solicitar tokens de acesso diretamente do servidor de autorização. Você precisa decidir como isso será feito, incluindo o tipo de concessão.

Configurar o ONTAP

Há várias tarefas de configuração do ONTAP que você precisa executar.

Defina funções REST e usuários locais

Com base na sua configuração de autorização, pode ser utilizado o processamento de identificação local do ONTAP. Nesse caso, você precisa revisar e definir as funções REST e as definições de usuário. E, dependendo do seu servidor de autorização, isso também pode incluir a administração de grupos com base nos valores UUID.

Configuração central

Há três etapas principais necessárias para executar a configuração principal do ONTAP, incluindo:

- Opcionalmente, instale o certificado raiz (e quaisquer certificados intermediários) para a CA que assinou o certificado do servidor de autorização.
- Defina o servidor de autorização.
- Ative o processamento OAuth 2,0 para o cluster.

Implantar o OAuth 2,0 no ONTAP

A implantação da funcionalidade principal do OAuth 2,0 envolve três etapas principais.

Antes de começar

Você deve se preparar para a implantação do OAuth 2,0 antes de configurar o ONTAP. Por exemplo, você precisa avaliar o servidor de autorização, incluindo como seu certificado foi assinado e se está atrás de um firewall. Consulte "Prepare-se para implantar o OAuth 2,0 com o ONTAP" para obter mais informações.

Etapa 1: Instale os certificados de CA raiz do servidor de autorização

O ONTAP inclui um grande número de certificados de CA raiz pré-instalados. Assim, em muitos casos, o certificado para o seu servidor de autorização será imediatamente reconhecido pelo ONTAP sem configuração adicional. Mas dependendo de como o certificado do servidor de autorização foi assinado, talvez seja necessário instalar um certificado de CA raiz e quaisquer certificados intermediários.

Siga as instruções fornecidas abaixo para instalar o certificado, se necessário. Você deve instalar todos os certificados necessários no nível do cluster.

Escolha o procedimento correto com base em como você acessa o ONTAP.

Exemplo 22. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em → ao lado de **certificados**.
4. Na guia **autoridades de certificação confiáveis**, clique em **Adicionar**.
5. Clique em **Importar** e selecione o arquivo de certificado.
6. Complete os parâmetros de configuração para o seu ambiente.
7. Clique em **Add**.

CLI

1. Inicie a instalação:

   ```
   security certificate install -type server-ca
   ```

2. Procure a seguinte mensagem do console:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Abra o arquivo de certificado com um editor de texto.
4. Copie o certificado inteiro, incluindo as seguintes linhas:

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. Cole o certificado no terminal após o prompt de comando.
6. Pressione **Enter** para concluir a instalação.
7. Confirme se o certificado está instalado usando uma das seguintes opções:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Etapa 2: Configurar o servidor de autorização

Você precisa definir pelo menos um servidor de autorização para o ONTAP. Você deve escolher os valores de parâmetro com base em sua configuração e plano de implantação. Reveja "Cenários de implantação do OAuth2" para determinar os parâmetros exatos necessários para a sua configuração.

Para modificar uma definição de servidor de autorização, você pode excluir a definição existente e criar uma nova.

O exemplo fornecido abaixo é baseado no primeiro cenário de implantação simples em "Validação local". Escopos auto-contidos são usados sem um proxy.

Escolha o procedimento correto com base em como você acessa o ONTAP. O procedimento CLI usa variáveis simbólicas que você precisa substituir antes de emitir o comando.

Exemplo 23. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em *** ao lado de *autorização OAuth 2,0**.
4. Selecione **mais opções**.
5. Forneça os valores necessários para sua implantação, como:
   - Nome
   - Aplicação (http)
   - URI do provedor JWKS
   - URI do emissor
6. Clique em **Add**.

CLI

1. Crie a definição novamente:

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Por exemplo:

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Passo 3: Ative o OAuth 2,0

O passo final é habilitar o OAuth 2,0. Esta é uma configuração global para o cluster ONTAP.

> Não ative o processamento do OAuth 2,0 até confirmar que o ONTAP, os servidores de autorização e quaisquer serviços de suporte foram configurados corretamente.

Escolha o procedimento correto com base em como você acessa o ONTAP.

Exemplo 24. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em → ao lado de **autorização OAuth 2,0**.
4. Ativar **autorização OAuth 2,0**.

CLI

1. Ativar OAuth 2,0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirmar que o OAuth 2,0 está ativado:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Emita uma chamada de API REST usando o OAuth 2,0

A implementação do OAuth 2,0 no ONTAP suporta aplicações cliente API REST. Você pode emitir uma simples chamada de API REST usando curl para começar a usar o OAuth 2,0. O exemplo apresentado abaixo recupera a versão do cluster do ONTAP.

Antes de começar

Você deve configurar e ativar o recurso OAuth 2,0 para seu cluster ONTAP. Isso inclui a definição de um servidor de autorização.

Passo 1: Adquira um token de acesso

Você precisa adquirir um token de acesso para usar com a chamada API REST. A solicitação de token é realizada fora do ONTAP e o procedimento exato depende do servidor de autorização e de sua configuração. Você pode solicitar o token através de um navegador da Web, com um comando curl ou usando uma linguagem de programação.

Para fins de ilustração, um exemplo de como um token de acesso pode ser solicitado ao Keycloak usando curl é apresentado abaixo.

Exemplo de capa-chave

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Você deve copiar e salvar o token retornado.

Etapa 2: Emita a chamada da API REST

Depois de ter um token de acesso válido, você pode usar um comando curl com o token de acesso para emitir uma chamada de API REST.

Parâmetros e variáveis

As duas variáveis no exemplo curl são descritas na tabela abaixo.

Variável	Descrição
FQDN_IP	O nome de domínio totalmente qualificado ou o endereço IP do LIF de gerenciamento do ONTAP.
ACCESS_TOKEN	O token de acesso OAuth 2,0 emitido pelo servidor de autorização.

Você deve primeiro definir essas variáveis no ambiente de shell Bash antes de emitir o exemplo curl. Por exemplo, na CLI do Linux digite o seguinte comando para definir e exibir a variável FQDN:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Depois que ambas as variáveis são definidas no seu shell Bash local, você pode copiar o comando curl e colá-lo na CLI. Pressione **Enter** para substituir as variáveis e emitir o comando.

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

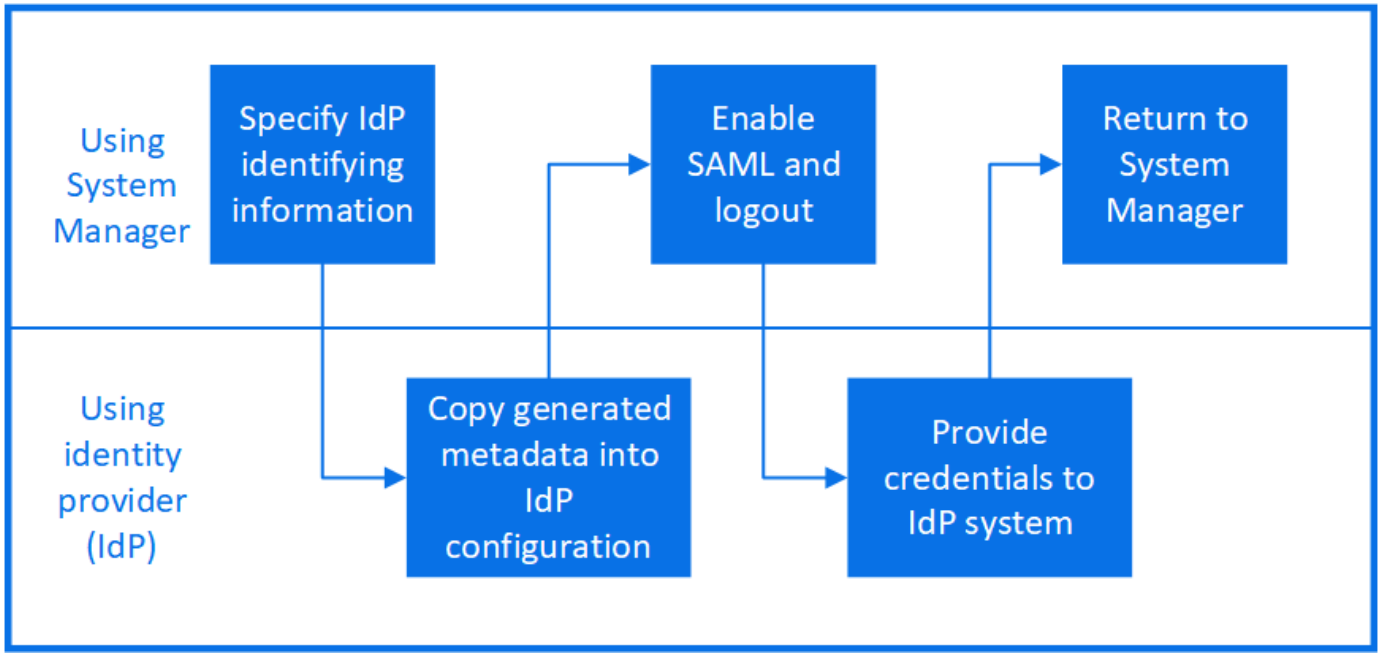
Configurar a autenticação SAML

A partir do ONTAP 9.3, você pode configurar a autenticação de linguagem de marcação de asserção de Segurança (SAML) para serviços da Web. Quando a autenticação SAML é configurada e ativada, os usuários são autenticados por um Provedor de identidade (IDP) externo em vez dos provedores de serviços de diretório, como o ative Directory e o LDAP.

Ativar a autenticação SAML

Para ativar a autenticação SAML com o System Manager ou com a CLI, execute as seguintes etapas. Se o cluster estiver executando o ONTAP 9.7 ou anterior, as etapas do Gerenciador de sistema que você precisa seguir serão diferentes. Consulte a ajuda online do System Manager disponível no seu sistema.

> Depois de ativar a autenticação SAML, somente usuários remotos podem acessar a GUI do System Manager. Os usuários locais não podem acessar a GUI do System Manager depois que a autenticação SAML estiver ativada.



Antes de começar

- O IDP que pretende utilizar para autenticação remota tem de ser configurado.

  > Consulte a documentação fornecida pelo IDP que você configurou.

- Você deve ter o URI do IDP.

Sobre esta tarefa

- A autenticação SAML aplica-se apenas `http` aos aplicativos e `ontapi`.

`http`Os aplicativos e `ontapi` são usados pelos seguintes serviços da Web: Infraestrutura do processador de serviço, APIs do ONTAP ou Gerenciador de sistema.

- A autenticação SAML é aplicável apenas para acessar o SVM admin.

Os seguintes IDPs foram validados com o System Manager:

- Serviços de Federação do ative Directory
- Cisco Duo (validado com as seguintes versões do ONTAP:)
  - 9.7P21 e versões posteriores do 9,7 (consulte a "Documentação do System Manager Classic")
  - 9.8P17 e versões posteriores do 9,8
  - 9,9.1P13 e versões posteriores do 9,9
  - 9.10.1P9 e versões posteriores do 9,10
  - 9.11.1P4 e versões posteriores do 9,11
  - 9.12.1 e versões posteriores
- Shibboleth

Execute as seguintes etapas, dependendo do ambiente:

Exemplo 25. Passos

System Manager

1. Clique em **Cluster > Settings**.
2. Ao lado de **Autenticação SAML**, clique em .
3. Verifique se há uma verificação na caixa de seleção **Ativar autenticação SAML**.
4. Insira o URL do URI de IDP (incluindo "https://").
5. Modifique o endereço do sistema host, se necessário.
6. Certifique-se de que está a ser utilizado o certificado correto:
   - Se o seu sistema foi mapeado com apenas um certificado com o tipo "servidor", esse certificado é considerado o padrão e não é exibido.
   - Se o seu sistema foi mapeado com vários certificados como tipo "servidor", um dos certificados será exibido. Para selecionar um certificado diferente, clique em **alterar**.
7. Clique em **Salvar**. Uma janela de confirmação exibe as informações de metadados, que foram copiadas automaticamente para a área de transferência.
8. Vá para o sistema IDP que você especificou e copie os metadados da área de transferência para atualizar os metadados do sistema.
9. Retorne à janela de confirmação (no System Manager) e marque a caixa de seleção **Eu configurei o IDP com o URI do host ou metadados**.
10. Clique em **Logout** para ativar a autenticação baseada em SAML. O sistema IDP exibirá uma tela de autenticação.
11. No sistema IDP, insira suas credenciais baseadas em SAML. Depois que suas credenciais forem verificadas, você será direcionado para a página inicial do System Manager.

CLI

1. Crie uma configuração SAML para que o ONTAP possa acessar os metadados do IDP:

   `security saml-sp create -idp-uri` *`idp_uri`* `-sp-host` *`ontap_host_name`*

   `idp_uri` É o endereço FTP ou HTTP do host IDP de onde os metadados IDP podem ser baixados.

   `ontap_host_name` É o nome do host ou endereço IP do host do provedor de serviços SAML, que neste caso é o sistema ONTAP. Por padrão, o endereço IP do LIF de gerenciamento de cluster é usado.

   Opcionalmente, você pode fornecer as informações do certificado do servidor ONTAP. Por padrão, as informações de certificado do servidor Web do ONTAP são usadas.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the Data ONTAP user configuration.
```

O URL para acessar os metadados do host do ONTAP é exibido.

2. No host IDP, configure o IDP com os metadados do host ONTAP.

   Para obter mais informações sobre como configurar o IDP, consulte a documentação do IDP.

3. Ativar configuração SAML:

   security saml-sp modify -is-enabled true

   Qualquer usuário existente que acesse o `http` aplicativo ou `ontapi` é configurado automaticamente para autenticação SAML.

4. Se você quiser criar usuários para o `http` aplicativo ou `ontapi` depois que o SAML for configurado, especifique SAML como o método de autenticação para os novos usuários.

   a. Criar um método de login para novos usuários com autenticação SAML
   security login create -user-or-group-name *user_name* -application [http | ontapi] -authentication-method saml -vserver *svm_name*

   ```
   cluster_12::> security login create -user-or-group-name admin1
   -application http -authentication-method saml -vserver
   cluster_12
   ```

   b. Verifique se a entrada do usuário foi criada:

   security login show

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no
none
admin          http        password      admin            no
none
admin          http        saml          admin            -
none
admin          ontapi      password      admin            no
none
admin          ontapi      saml          admin            -
none
admin          service-processor
                           password      admin            no
none
admin          ssh         password      admin            no
none
admin1         http        password      backup           no
none
**admin1       http        saml          backup           -
none**
```

Desativar a autenticação SAML

Você pode desativar a autenticação SAML quando quiser parar de autenticar usuários da Web usando um provedor de identidade externo (IDP). Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ative Directory e o LDAP, são usados para autenticação.

Execute as seguintes etapas, dependendo do ambiente:

Exemplo 26. Passos

System Manager

1. Clique em **Cluster > Settings**.
2. Em **Autenticação SAML**, clique no botão de alternância **Enabled**.
3. *Opcional*: Você também pode clicar ⚙ ao lado de **Autenticação SAML** e, em seguida, desmarcar a caixa de seleção **Ativar autenticação SAML**.

CLI

1. Desativar autenticação SAML:

   ```
   security saml-sp modify -is-enabled false
   ```

2. Se você não quiser mais usar a autenticação SAML ou se quiser modificar o IDP, exclua a configuração SAML:

   ```
   security saml-sp delete
   ```

Solucionar problemas com a configuração SAML

Se a configuração da autenticação SAML (Security Assertion Markup Language) falhar, você poderá reparar manualmente cada nó em que a configuração SAML falhou e recuperar da falha. Durante o processo de reparo, o servidor da Web é reiniciado e todas as conexões HTTP ou HTTPS ativas são interrompidas.

Sobre esta tarefa

Quando você configura a autenticação SAML, o ONTAP aplica a configuração SAML por nó. Quando você ativa a autenticação SAML, o ONTAP tenta reparar automaticamente cada nó se houver problemas de configuração. Se houver problemas com a configuração SAML em qualquer nó, você poderá desabilitar a autenticação SAML e rehabilitar a autenticação SAML. Pode haver situações em que a configuração SAML não se aplica em um ou mais nós, mesmo após a reativação da autenticação SAML. Você pode identificar o nó no qual a configuração SAML falhou e, em seguida, reparar manualmente esse nó.

Passos

1. Inicie sessão no nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Identificar o nó no qual a configuração SAML falhou:

   ```
   security saml-sp status show -instance
   ```

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

3. Repare a configuração SAML no nó com falha:

   security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   O servidor web é reiniciado e quaisquer conexões HTTP ou HTTPS ativas são interrompidas.

4. Verifique se o SAML está configurado com êxito em todos os nós:

   security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                 Update Status: **config-success**
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

Informações relacionadas

"Referência do comando ONTAP"

Autenticação e autorização usando WebAuthn MFA

Visão geral da autenticação multifator WebAuthn

A partir do ONTAP 9.16,1, os administradores podem ativar a autenticação multifator WebAuthn (MFA) para usuários que fazem login no Gerenciador de sistema. Isso permite logins do System Manager usando uma chave FIDO2 (como uma YubiKey) como uma segunda forma de autenticação. Por padrão, o WebAuthn MFA está desativado para usuários novos e existentes do ONTAP.

O WebAuthn MFA é compatível com usuários e grupos que usam os seguintes tipos de autenticação para o primeiro método de autenticação:

- Usuários: Senha, domínio ou nsswitch
- Grupos: Domínio ou nsswitch

Depois de ativar o WebAuthn MFA como o segundo método de autenticação para um usuário, o usuário é solicitado a Registrar um autenticador de hardware ao fazer login no System Manager. Após o Registro, a chave privada é armazenada no autenticador e a chave pública é armazenada no ONTAP.

O ONTAP suporta uma credencial WebAuthn por usuário. Se um usuário perder um autenticador e precisar substituí-lo, o administrador do ONTAP precisará excluir a credencial WebAuthn do usuário para que o usuário possa Registrar um novo autenticador no próximo login.

Os usuários que têm o WebAuthn MFA habilitado como um segundo método de autenticação precisam usar o FQDN (por exemplo, "https://myontap.example.com") em vez do endereço IP (por exemplo, "https://192.168.100.200") para acessar o System Manager. Para usuários com WebAuthn MFA habilitado, as tentativas de fazer login no System Manager usando o endereço IP são rejeitadas.

Habilite o MFA WebAuthn para usuários ou grupos do Gerenciador de sistema do ONTAP

Como administrador do ONTAP, você pode ativar o WebAuthn MFA para um usuário ou grupo do Gerenciador de sistema adicionando um novo usuário ou grupo com a opção de WebAuthn MFA ativada ou habilitando a opção para um usuário ou grupo existente.

Depois de ativar o WebAuthn MFA como o segundo método de autenticação para um usuário ou grupo, o usuário (ou todos os usuários desse grupo) será solicitado a Registrar um dispositivo FIDO2 de hardware no próximo login no System Manager. Esse Registro é gerenciado pelo sistema operacional local do usuário e geralmente consiste em inserir a chave de segurança, criar uma chave de acesso e tocar na chave de segurança (se suportada).

Ative o WebAuthn MFA ao criar um novo usuário ou grupo

Você pode criar um novo usuário ou grupo com o WebAuthn MFA habilitado usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Selecione **Adicionar** em **usuários**.
4. Especifique um nome de usuário ou grupo e selecione uma função no menu suspenso para **função**.
5. Especifique um método de login e uma senha para o usuário ou grupo.

   WebAuthn MFA suporta métodos de login de "senha", "domínio" ou "nsswitch" para usuários e "domínio" ou "nsswitch" para grupos.

6. Na coluna **MFA para HTTP**, selecione **Enabled**.
7. Selecione **Guardar**.

CLI

1. Crie um novo usuário ou grupo com o WebAuthn MFA habilitado.

   No exemplo a seguir, o WebAuthn MFA é habilitado escolhendo "publikey" para o segundo método de autenticação:

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Ative o WebAuthn MFA para um usuário ou grupo existente

Você pode ativar o WebAuthn MFA para um usuário ou grupo existente.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de utilizadores e grupos, selecione o menu de opções para o utilizador ou grupo que pretende editar.

   WebAuthn MFA suporta métodos de login de "senha", "domínio" ou "nsswitch" para usuários e "domínio" ou "nsswitch" para grupos.
4. Na coluna **MFA para HTTP** para esse usuário, selecione **Enabled**.
5. Selecione **Guardar**.

CLI

1. Modifique um usuário ou grupo existente para ativar o WebAuthn MFA para esse usuário ou grupo.

   No exemplo a seguir, o WebAuthn MFA é habilitado escolhendo "publikey" para o segundo método de autenticação:

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "login de segurança criar"
- "modificação de início de sessão de segurança"

Desative o WebAuthn MFA para usuários do Gerenciador de sistema do ONTAP

Como administrador do ONTAP, você pode desativar o WebAuthn MFA para um usuário ou grupo editando o usuário ou grupo com o Gerenciador do sistema ou a CLI do ONTAP.

Desative o WebAuthn MFA para um usuário ou grupo existente

Você pode desativar o WebAuthn MFA para um usuário ou grupo existente a qualquer momento.

> Se desativar as credenciais registadas, as credenciais são retidas. Se você ativar as credenciais novamente no futuro, as mesmas credenciais serão usadas, para que o usuário não precise se Registrar novamente ao fazer login.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de utilizadores e grupos, selecione o utilizador ou grupo que pretende editar.
4. Na coluna **MFA para HTTP** para esse usuário, selecione **Disabled**.
5. Selecione **Guardar**.

CLI

1. Modifique um usuário ou grupo existente para desativar o WebAuthn MFA para esse usuário ou grupo.

   No exemplo a seguir, o WebAuthn MFA é desativado escolhendo "nenhum" para o segundo método de autenticação.

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method none \
                      -application http \
                      -role admin
```

Saiba mais

Visite as páginas do manual do ONTAP para este comando:

- "modificação de início de sessão de segurança"

Veja as configurações de MFA do ONTAP WebAuthn e gerencie credenciais

Como administrador do ONTAP, você pode exibir configurações de MFA WebAuthn em todo o cluster e gerenciar credenciais de usuário e grupo para o MFA WebAuthn.

Exibir configurações de cluster para WebAuthn MFA

Você pode exibir as configurações de cluster para WebAuthn MFA usando a CLI do ONTAP.

Passos

1. Veja as configurações do cluster para WebAuthn MFA. Opcionalmente, você pode especificar uma VM de armazenamento usando o `vserver` argumento:

```
security webauthn show -vserver <storage_vm_name>
```

Veja algoritmos de chave pública suportados do WebAuthn MFA

Você pode exibir os algoritmos de chave pública compatíveis para WebAuthn MFA para uma VM de

armazenamento ou para um cluster.

Passos

1. Liste os algoritmos de chave pública suportados do WebAuthn MFA. Opcionalmente, você pode especificar uma VM de armazenamento usando o `vserver` argumento:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Veja as credenciais do WebAuthn MFA registradas

Como administrador do ONTAP, você pode exibir as credenciais de WebAuthn registradas para todos os usuários. Os utilizadores não administradores que utilizam este procedimento só podem ver as suas próprias credenciais WebAuthn registadas.

Passos

1. Veja as credenciais do WebAuthn MFA registradas:

```
security webauthn credentials show
```

Remova uma credencial WebAuthn MFA registrada

Você pode remover uma credencial WebAuthn MFA registrada. Isso é útil quando a chave de hardware de um usuário foi perdida, roubada ou não está mais em uso. Você também pode remover uma credencial registrada quando o usuário ainda tem o autenticador de hardware original, mas deseja substituí-la por uma nova. Depois de remover a credencial, o usuário será solicitado a Registrar o autenticador de substituição.

> ⓘ A remoção de uma credencial registrada para um usuário não desativa o WebAuthn MFA para o usuário. Se um usuário perder um autenticador de hardware e precisar fazer login antes de substituí-lo, você precisará remover a credencial usando estas etapas e também "Desative o WebAuthn MFA" para o usuário.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de usuários e grupos, selecione o menu de opções para o usuário ou grupo cujas credenciais deseja remover.
4. Selecione **Remover MFA para credenciais HTTP**.
5. Selecione **Remover**.

CLI

1. Elimine as credenciais registadas. Observe o seguinte:
   - Opcionalmente, você pode especificar uma VM de storage do usuário. Se omitida, a credencial é removida no nível do cluster.
   - Opcionalmente, você pode especificar um nome de usuário do usuário para o qual você está excluindo a credencial. Se omitida, a credencial é removida para o usuário atual.

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "segurança webauthn show"
- "os algoritmos suportados por webauthn de segurança são mostrados"
- "credenciais webauthn de segurança são exibidas"
- "credenciais de segurança webauthn excluídas"

Gerenciar serviços da Web

Gerencie a visão geral dos serviços da Web

Você pode ativar ou desativar um serviço da Web para o cluster ou uma máquina virtual de armazenamento (SVM), exibir as configurações de serviços da Web e controlar se os usuários de uma função podem acessar um serviço da Web.

Você pode gerenciar os serviços da Web para o cluster ou uma SVM das seguintes maneiras:

- Ativar ou desativar um serviço Web específico
- Especificar se o acesso a um serviço da Web é restrito apenas a HTTP encriptado (SSL)
- Exibindo a disponibilidade de serviços da Web
- Permitir ou não permitir que usuários de uma função acessem um serviço da Web
- Exibindo as funções que têm permissão para acessar um serviço da Web

Para que um usuário acesse um serviço da Web, todas as seguintes condições devem ser atendidas:

- O usuário deve ser autenticado.

  Por exemplo, um serviço da Web pode solicitar um nome de usuário e uma senha. A resposta do usuário deve corresponder a uma conta válida.

- O utilizador tem de ser configurado com o método de acesso correto.

  A autenticação só é bem-sucedida para os usuários com o método de acesso correto para o serviço web fornecido. Para o serviço Web da API ONTAP `ontapi`), os usuários devem ter o `ontapi` método de acesso. Para todos os outros serviços da Web, os usuários devem ter o `http` método de acesso.

  > Você usa os `security login` comandos para gerenciar os métodos de acesso e os métodos de autenticação dos usuários.

- O serviço Web deve ser configurado para permitir a função de controle de acesso do usuário.

  > Você usa os `vserver services web access` comandos para controlar o acesso de uma função a um serviço da Web.

Se um firewall estiver ativado, a política de firewall para o LIF a ser usado para serviços da Web deve ser configurada para permitir HTTP ou HTTPS.

Se você usar HTTPS para acesso ao serviço da Web, o SSL para o cluster ou SVM que ofereça o serviço da Web também deverá estar habilitado e fornecer um certificado digital para o cluster ou SVM.

Gerencie o acesso a serviços da Web

Um serviço da Web é um aplicativo que os usuários podem acessar usando HTTP ou HTTPS. O administrador do cluster pode configurar o mecanismo de protocolo da Web, configurar SSL, ativar um serviço da Web e permitir que os utilizadores de uma função acedam a um serviço da Web.

A partir do ONTAP 9.6, são suportados os seguintes serviços Web:

- Infraestrutura do processador de serviço (`spi`)

  Esse serviço torna os arquivos de log, despejo de núcleo e MIB de um nó disponíveis para acesso HTTP ou HTTPS por meio do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó. A predefinição é `enabled`.

  Após uma solicitação para acessar os arquivos de log de um nó ou arquivos de despejo de núcleo, o `spi` serviço da Web cria automaticamente um ponto de montagem de um nó para o volume raiz de outro nó onde os arquivos residem. Não é necessário criar manualmente o ponto de montagem. "

- APIs do ONTAP (`ontapi`)

  Este serviço permite executar APIs do ONTAP para executar funções administrativas com um programa remoto. A predefinição é `enabled`.

  Este serviço pode ser necessário para algumas ferramentas de gerenciamento externas. Por exemplo, se

você usar o System Manager, você deve deixar esse serviço habilitado.

- Descoberta do Data ONTAP (`disco`)

  Este serviço permite que os aplicativos de gerenciamento off-box descubram o cluster na rede. A predefinição é `enabled`.

- Diagnóstico de suporte (`supdiag`)

  Este serviço controla o acesso a um ambiente privilegiado no sistema para auxiliar na análise e resolução de problemas. A predefinição é `disabled`. Você deve habilitar este serviço somente quando direcionado pelo suporte técnico.

- System (`sysmgr`Manager)

  Esse serviço controla a disponibilidade do Gerenciador de sistema, que está incluído no ONTAP. A predefinição é `enabled`. Este serviço é suportado apenas no cluster.

- Atualização do controlador de gerenciamento de placa base (BMC) de firmware (`FW_BMC`)

  Este serviço permite-lhe transferir ficheiros de firmware do BMC. A predefinição é `enabled`.

- Documentação do ONTAP (`docs`)

  Este serviço fornece acesso à documentação do ONTAP. A predefinição é `enabled`.

- APIs RESTful do ONTAP (`docs_api`)

  Este serviço fornece acesso à documentação da API RESTful do ONTAP. A predefinição é `enabled`.

- Carregar e transferir ficheiros (`fud`)

  Este serviço oferece upload e download de arquivos. A predefinição é `enabled`.

- Mensagens do ONTAP (`ontapmsg`)

  Este serviço suporta uma interface de publicação e assinatura, permitindo que você se inscreva em eventos. A predefinição é `enabled`.

- Portal do ONTAP (`portal`)

  Este serviço implementa o gateway em um servidor virtual. A predefinição é `enabled`.

- Interface ONTAP RESTful (`rest`)

  Esse serviço dá suporte a uma interface RESTful que é usada para gerenciar remotamente todos os elementos da infraestrutura do cluster. A predefinição é `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  Este serviço fornece recursos para dar suporte ao provedor de serviços SAML. A predefinição é `enabled`.

- Fornecedor de serviços SAML (`saml-sp`)

Esse serviço oferece serviços como metadados SP e o serviço de asserção ao consumidor para o provedor de serviços. A predefinição é `enabled`.

A partir do ONTAP 9.7, são suportados os seguintes serviços adicionais:

- Arquivos de backup de (`backups`configuração)

  Este serviço permite-lhe transferir ficheiros de cópia de segurança de configuração. A predefinição é `enabled`.

- Segurança do ONTAP (`security`)

  Este serviço suporta o gerenciamento de token CSRF para autenticação aprimorada. A predefinição é `enabled`.

Gerencie o mecanismo de protocolo da Web

Você pode configurar o mecanismo de protocolo da Web no cluster para controlar se o acesso à Web é permitido e quais versões SSL podem ser usadas. Também pode apresentar as definições de configuração do motor de protocolo Web.

Você pode gerenciar o mecanismo de protocolo da Web no nível do cluster das seguintes maneiras:

- Você pode especificar se os clientes remotos podem usar HTTP ou HTTPS para acessar o conteúdo do serviço da Web usando o `system services web modify` comando com o `-external` parâmetro.
- Você pode especificar se SSLv3 deve ser usado para acesso seguro à Web usando o `security config modify` comando com o `-supported-protocol` parâmetro. Por padrão, o SSLv3 está desativado. Transport Layer Security 1,0 (TLSv1,0) está ativado e pode ser desativado se necessário.
- Você pode ativar o modo de conformidade FIPS (Federal Information Processing Standard) 140-2 para interfaces de serviço da Web do plano de controle em todo o cluster.

  Por padrão, o modo de conformidade com o FIPS 140-2 está desativado.

  - **Quando o modo de conformidade com o FIPS 140-2 estiver desativado**, é possível ativar o modo de conformidade com o FIPS 140-2 definindo o `is-fips-enabled` parâmetro como `true` para `security config modify` o comando e, em seguida, usando o `security config show` comando para confirmar o status on-line.
  - **Quando o modo de conformidade com o FIPS 140-2 estiver ativado**
    - A partir do ONTAP 9.11,1, TLSv1, TLSv1,1 e SSLv3 estão desativados e apenas TSLv1,2 e TSLv1,3 permanecem ativados. Afeta outros sistemas e comunicações que são internos e externos ao ONTAP 9. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativar, TLSv1, TLSv1,1 e SSLv3 permanecerão desativados. O TLSv1,2 ou o TLSv1,3 permanecerão ativados dependendo da configuração anterior.
    - Para versões do ONTAP anteriores a 9.11.1, tanto o TLSv1 como o SSLv3 estão desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando o modo de conformidade FIPS 140-2 estiver ativado. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativá-lo, o TLSv1 e o SSLv3 permanecerão desativados, mas o TLSv1,2 ou o TLSv1,1 e o TLSv1,2 serão ativados dependendo da configuração anterior.

- Você pode exibir a configuração de segurança em todo o cluster usando o `system security config show` comando.

Se o firewall estiver ativado, a política de firewall para a interface lógica (LIF) a ser usada para serviços da Web deve ser configurada para permitir o acesso HTTP ou HTTPS.

Se você usar HTTPS para acesso ao serviço da Web, o SSL para o cluster ou a máquina virtual de armazenamento (SVM) que ofereça o serviço da Web também deverá estar habilitado e fornecer um certificado digital para o cluster ou SVM.

Nas configurações do MetroCluster, as alterações de configuração feitas para o mecanismo de protocolo da Web em um cluster não são replicadas no cluster de parceiros.

Comandos para gerenciar o mecanismo de protocolo da Web

Você usa os `system services web` comandos para gerenciar o mecanismo de protocolo da Web. Use os `system services firewall policy create` comandos e `network interface modify` para permitir que as solicitações de acesso à Web passem pelo firewall.

Se você quiser…	Use este comando…
Configure o mecanismo de protocolo da Web no nível do cluster: • Ative ou desative o mecanismo de protocolo da Web para o cluster • Ative ou desative o SSLv3 para o cluster • Ativar ou desativar a conformidade com o FIPS 140-2 para serviços Web seguros (HTTPS)	`system services web modify`
Exibir a configuração do mecanismo de protocolo da Web no nível do cluster, determinar se os protocolos da Web estão funcionais em todo o cluster e exibir se a conformidade com o FIPS 140-2 está ativada e on-line	`system services web show`
Exibir a configuração do mecanismo de protocolo da Web no nível do nó e a atividade de manipulação de serviços da Web para os nós no cluster	`system services web node show`
Crie uma política de firewall ou adicione um serviço de protocolo HTTP ou HTTPS a uma política de firewall existente para permitir que as solicitações de acesso à Web passem pelo firewall	`system services firewall policy create` Definir o `-service` parâmetro para `http` ou `https` permite que as solicitações de acesso à Web passem pelo firewall.

Se você quiser…	Use este comando…
Associar uma política de firewall a um LIF	`network interface modify` Você pode usar o `-firewall-policy` parâmetro para modificar a política de firewall de um LIF.

Configurar o acesso aos serviços da Web

A configuração do acesso a serviços da Web permite que usuários autorizados usem HTTP ou HTTPS para acessar o conteúdo do serviço no cluster ou em uma máquina virtual de armazenamento (SVM).

Passos

1. Se um firewall estiver ativado, verifique se o acesso HTTP ou HTTPS está configurado na política de firewall para o LIF que será usado para serviços da Web:

   Você pode verificar se um firewall está habilitado usando o `system services firewall show` comando.

   a. Para verificar se HTTP ou HTTPS está configurado na política de firewall, use o `system services firewall policy show` comando.

      Você define o `-service` parâmetro `system services firewall policy create` do comando para `http` ou `https` para ativar a diretiva para oferecer suporte ao acesso à Web.

   b. Para verificar se a política de firewall que suporta HTTP ou HTTPS está associada ao LIF que fornece serviços da Web, use o `network interface show` comando com o `-firewall-policy` parâmetro.

      Você usa o `network interface modify` comando com o `-firewall-policy` parâmetro para colocar a política de firewall em vigor para um LIF.

2. Para configurar o mecanismo de protocolo da Web em nível de cluster e tornar o conteúdo do serviço da Web acessível, use o `system services web modify` comando.
3. Se você planeja usar serviços da Web seguros (HTTPS), ative o SSL e forneça informações de certificado digital para o cluster ou SVM usando o `security ssl modify` comando.
4. Para ativar um serviço da Web para o cluster ou SVM, use o `vserver services web modify` comando.

   Repita essa etapa para cada serviço que você deseja habilitar para o cluster ou SVM.

5. Para autorizar uma função a acessar serviços da Web no cluster ou SVM, use o `vserver services web access create` comando.

   A função que você concede acesso já deve existir. Você pode exibir funções existentes usando o `security login role show` comando ou criar novas funções usando o `security login role create` comando.

6. Para uma função que tenha sido autorizada a acessar um serviço da Web, verifique se seus usuários

também estão configurados com o método de acesso correto, verificando a saída do `security login show` comando.

Para acessar o serviço Web da API ONTAP `ontapi`), um usuário deve ser configurado com o `ontapi` método de acesso. Para acessar todos os outros serviços da Web, um usuário deve ser configurado com o `http` método de acesso.

Use o `security login create` comando para adicionar um método de acesso a um usuário.

Comandos para gerenciar serviços da Web

Use os `vserver services web` comandos para gerenciar a disponibilidade de serviços da Web para o cluster ou uma máquina virtual de storage (SVM). Você usa os `vserver services web access` comandos para controlar o acesso de uma função a um serviço da Web.

Se você quiser…	Use este comando…
Configurar um serviço da Web para o cluster ou anSVM: • Ativar ou desativar um serviço Web • Especifique se apenas o HTTPS pode ser usado para acessar um serviço da Web	`vserver services web modify`
Exibir a configuração e a disponibilidade dos serviços da Web para o cluster ou anSVM	`vserver services web show`
Autorizar uma função a acessar um serviço da Web no cluster ou na anSVM	`vserver services web access create`
Exibir as funções autorizadas a acessar serviços da Web no cluster ou no anSVM	`vserver services web access show`
Impedir que uma função acesse um serviço da Web no cluster ou na anSVM	`vserver services web access delete`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar pontos de montagem nos nós

O `spi` serviço da Web cria automaticamente um ponto de montagem de um nó para o volume raiz de outro nó, mediante uma solicitação para acessar os arquivos de log ou arquivos centrais do nó. Embora você não precise gerenciar manualmente pontos de montagem, você pode fazê-lo usando os `system node root-mount` comandos.

Se você quiser…	Use este comando…
Crie manualmente um ponto de montagem de um nó para o volume raiz de outro nó	`system node root-mount create` Apenas um único ponto de montagem pode existir de um nó para outro.
Exiba pontos de montagem existentes nos nós do cluster, incluindo o tempo em que um ponto de montagem foi criado e seu estado atual	`system node root-mount show`
Exclua um ponto de montagem de um nó para o volume raiz de outro nó e force as conexões ao ponto de montagem para fechar	`system node root-mount delete`

Informações relacionadas

"Referência do comando ONTAP"

Gerenciar SSL

Use os `security ssl` comandos para gerenciar o protocolo SSL para o cluster ou uma máquina virtual de armazenamento (SVM). O protocolo SSL melhora a segurança do acesso à Web usando um certificado digital para estabelecer uma conexão criptografada entre um servidor da Web e um navegador.

Você pode gerenciar SSL para o cluster ou uma máquina virtual de armazenamento (SVM) das seguintes maneiras:

- Ativar SSL
- Gerar e instalar um certificado digital e associá-lo ao cluster ou SVM
- Exibindo a configuração SSL para ver se o SSL foi ativado e, se disponível, o nome do certificado SSL
- Configuração de políticas de firewall para o cluster ou SVM, para que as solicitações de acesso à Web possam passar
- Definir quais versões SSL podem ser usadas
- Restringindo o acesso apenas a solicitações HTTPS para um serviço da Web

Comandos para gerenciar SSL

Use os `security ssl` comandos para gerenciar o protocolo SSL para o cluster ou uma máquina virtual de armazenamento (SVM).

Se você quiser…	Use este comando…
Ative o SSL para o cluster ou um SVM e associe um certificado digital a ele	`security ssl modify`
Exiba a configuração SSL e o nome do certificado para o cluster ou um SVM	`security ssl show`

Solucionar problemas de acesso ao serviço da Web

Os erros de configuração causam problemas de acesso ao serviço da Web. Você pode resolver os erros garantindo que o LIF, a política de firewall, o mecanismo de protocolo da Web, os serviços da Web, os certificados digitais e a autorização de acesso do usuário estejam configurados corretamente.

A tabela a seguir ajuda a identificar e tratar erros de configuração do serviço da Web:

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
O navegador da Web retorna um `unable to connect` erro ou `failure to establish a connection` quando você tenta acessar um serviço da Web.	Seu LIF pode estar configurado incorretamente.	Certifique-se de que você pode fazer ping no LIF que fornece o serviço da Web. Você usa o `network ping` comando para fazer ping em um LIF. Para obter informações sobre a configuração de rede, consulte o *Network Management Guide*.
O firewall pode estar configurado incorretamente.	Certifique-se de que uma política de firewall esteja configurada para suportar HTTP ou HTTPS e que a política esteja atribuída ao LIF que fornece o serviço da Web. Você usa os `system services firewall policy` comandos para gerenciar políticas de firewall. Você usa o `network interface modify` comando com o `-firewall-policy` parâmetro para associar uma política a um LIF.	Seu mecanismo de protocolo da Web pode estar desativado.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que o mecanismo de protocolo da Web está ativado para que os serviços da Web estejam acessíveis. Você usa os `system services web` comandos para gerenciar o mecanismo de protocolo da Web para o cluster.	Seu navegador retorna um `not found` erro quando você tenta acessar um serviço da Web.	O serviço da Web pode estar desativado.
Certifique-se de que cada serviço Web ao qual você deseja permitir acesso esteja ativado individualmente. Você usa o `vserver services web modify` comando para habilitar um serviço da Web para acesso.	O navegador da Web não consegue fazer login em um serviço da Web com o nome de conta e a senha de um usuário.	O utilizador não pode ser autenticado, o método de acesso não está correto ou o utilizador não está autorizado a aceder ao serviço Web.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que a conta de utilizador existe e está configurada com o método de acesso e o método de autenticação corretos. Além disso, certifique-se de que a função do utilizador está autorizada a aceder ao serviço Web. Você usa os `security login` comandos para gerenciar contas de usuário e seus métodos de acesso e métodos de autenticação. Acessar o serviço da Web da API do ONTAP requer o `ontapi` método de acesso. O acesso a todos os outros serviços da Web requer o `http` método de acesso. Você usa os `vserver services web access` comandos para gerenciar o acesso de uma função a um serviço da Web.	Você se coneta ao serviço da Web com HTTPS e o navegador da Web indica que sua conexão foi interrompida.	Talvez você não tenha o SSL ativado no cluster ou na máquina virtual de armazenamento (SVM) que fornece o serviço da Web.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que o cluster ou SVM tenha SSL habilitado e que o certificado digital seja válido. Você usa os `security ssl` comandos para gerenciar a configuração SSL para servidores HTTP e o `security certificate show` comando para exibir informações de certificado digital.	Você se coneta ao serviço da Web com HTTPS e o navegador da Web indica que a conexão não é confiável.	Você pode estar usando um certificado digital autoassinado.

Verifique a identidade de servidores remotos usando certificados

Verifique a identidade de servidores remotos usando a visão geral de certificados

O ONTAP suporta recursos de certificado de segurança para verificar a identidade de servidores remotos.

O software ONTAP permite conexões seguras usando esses recursos e protocolos de certificado digital:

- O OCSP (Online Certificate Status Protocol) valida o status de solicitações de certificados digitais de serviços ONTAP usando conexões SSL e TLS (Transport Layer Security). Esta funcionalidade está desativada por predefinição.
- Um conjunto padrão de certificados raiz confiáveis é incluído no software ONTAP.
- Os certificados KMIP (Key Management Interoperability Protocol) permitem a autenticação mútua de um cluster e de um servidor KMIP.

Verifique se os certificados digitais são válidos usando OCSP

A partir do ONTAP 9.2, o protocolo OCSP (Online Certificate Status Protocol) permite que aplicativos ONTAP que usam comunicações TLS (Transport Layer Security) recebam status de certificado digital quando o OCSP está ativado. Você pode ativar ou desativar verificações de status do certificado OCSP para aplicativos específicos a qualquer momento. Por padrão, a verificação do status do certificado OCSP está desativada.

O que você vai precisar

Você precisa de acesso avançado ao nível de privilégio para executar esta tarefa.

Sobre esta tarefa

O OCSP suporta as seguintes aplicações:

- AutoSupport
- Sistema de Gestão de Eventos (EMS)
- LDAP em TLS
- Key Management Interoperability Protocol (KMIP)
- Registo de auditoria
- FabricPool
- SSH (começando com ONTAP 9.13,1)

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`.
2. Para ativar ou desativar as verificações de status do certificado OCSP para aplicativos ONTAP específicos, use o comando apropriado.

Se você quiser que as verificações de status do certificado OCSP para alguns aplicativos sejam…	Use o comando…
Ativado	`security config ocsp enable -app app name`
Desativado	`security config ocsp disable -app app name`

O seguinte comando permite o suporte OCSP para AutoSupport e EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Quando o OCSP está ativado, o aplicativo recebe uma das seguintes respostas:

- Bom - o certificado é válido e a comunicação prossegue.
- Revogado - o certificado é considerado permanentemente como não fidedigno pela Autoridade de Certificação de emissão e a comunicação não procede.
- Desconhecido - o servidor não tem nenhuma informação de estado sobre o certificado e a comunicação não consegue prosseguir.
- As informações do servidor OCSP estão ausentes no certificado - o servidor funciona como se o OCSP estivesse desativado e continua com a comunicação TLS, mas nenhuma verificação de status ocorre.
- Sem resposta do servidor OCSP - o aplicativo não consegue prosseguir.

3. Para ativar ou desativar as verificações de status do certificado OCSP para todos os aplicativos que usam comunicações TLS, use o comando apropriado.

Se você quiser que as verificações de status do certificado OCSP para todos os aplicativos sejam…	Use o comando…
Ativado	`security config ocsp enable -app all`
Desativado	`security config ocsp disable -app all`

Quando ativado, todos os aplicativos recebem uma resposta assinada, significando que o certificado especificado é bom, revogado ou desconhecido. No caso de um certificado revogado, o pedido não irá prosseguir. Se o aplicativo não receber uma resposta do servidor OCSP ou se o servidor estiver inacessível, o aplicativo não conseguirá prosseguir.

4. Use o `security config ocsp show` comando para exibir todos os aplicativos que suportam OCSP e seu status de suporte.

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true
         ssh                             true

         8 entries were displayed.
```

Exibir certificados padrão para aplicativos baseados em TLS

A partir do ONTAP 9.2, o ONTAP fornece um conjunto padrão de certificados raiz confiáveis para aplicativos ONTAP usando a Segurança da camada de Transporte (TLS).

O que você vai precisar

Os certificados padrão são instalados somente no SVM do administrador durante sua criação ou durante uma atualização para o ONTAP 9.2.

Sobre esta tarefa

Os aplicativos atuais que atuam como cliente e exigem validação de certificado são AutoSupport, EMS, LDAP, Registro de auditoria, FabricPool e KMIP.

Quando os certificados expiram, é invocada uma mensagem EMS que solicita ao utilizador que elimine os certificados. Os certificados padrão só podem ser excluídos no nível avançado de privilégio.

> A exclusão dos certificados padrão pode resultar em alguns aplicativos do ONTAP não funcionarem como esperado (por exemplo, AutoSupport e Registro de auditoria).

Passo

1. Você pode exibir os certificados padrão instalados no SVM do administrador usando o comando show do certificado de segurança:

   `security certificate show -vserver –type server-ca`

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

Autentique mutuamente o cluster e um servidor KMIP

Autenticando mutuamente o cluster e uma visão geral do servidor KMIP

Autenticar mutuamente o cluster e um gerenciador de chaves externo, como um servidor KMIP (Key Management Interoperability Protocol), permite que o gerenciador de chaves se comunique com o cluster usando KMIP em SSL. Você o faz quando um aplicativo ou uma determinada funcionalidade (por exemplo, a funcionalidade criptografia de armazenamento) exige chaves seguras para fornecer acesso seguro aos dados.

Gerar uma solicitação de assinatura de certificado para o cluster

Você pode usar o comando certificado de segurança `generate-csr` para gerar uma solicitação de assinatura de certificado (CSR). Depois de processar sua solicitação, a autoridade de certificação (CA) envia o certificado digital assinado.

O que você vai precisar

Você deve ser um administrador de cluster ou um administrador de SVM para executar essa tarefa.

Passos

1. Gerar um CSR:

   `security certificate generate-csr -common-name *FQDN_or_common_name* -size`

512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash -function SHA1|SHA256|MD5

Para obter a sintaxe completa do comando, consulte as páginas man.

O comando a seguir cria uma CSR com uma chave privada de 2.048 bits gerada pela função de hash SHA256 para uso pelo grupo Software no departamento DE TI de uma empresa cujo nome comum personalizado é server1.companyname.com, localizada em Sunnyvale, Califórnia, EUA. O endereço de e-mail do administrador de Contatos do SVM é web@example.com. O sistema apresenta a CSR e a chave privada na saída.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copie a solicitação de certificado da saída CSR e, em seguida, envie-a em formato eletrônico (como e-mail) para uma CA de terceiros confiável para assinatura.

   Após processar sua solicitação, a CA envia o certificado digital assinado. Você deve manter uma cópia da chave privada e do certificado digital assinado pela CA.

Instale um certificado de servidor assinado pela CA para o cluster

Para permitir que um servidor SSL autentique o cluster ou a máquina virtual de armazenamento (SVM) como um cliente SSL, instale um certificado digital com o tipo de cliente no cluster ou SVM. Em seguida, você fornece o certificado cliente-CA ao administrador do servidor SSL para instalação no servidor.

O que você vai precisar

Você já deve ter instalado o certificado raiz do servidor SSL no cluster ou SVM com o `server-ca` tipo de certificado.

Passos

1. Para usar um certificado digital autoassinado para autenticação de cliente, use o `security certificate create` comando com o `type client` parâmetro.
2. Para usar um certificado digital assinado pela CA para autenticação de cliente, execute as seguintes etapas:

   a. Gere uma solicitação de assinatura de certificado digital (CSR) usando o comando de certificado de segurança `generate-csr`.

      O ONTAP exibe a saída CSR, que inclui uma solicitação de certificado e uma chave privada, e lembra que você deve copiar a saída para um arquivo para referência futura.

   b. Envie a solicitação de certificado da saída CSR em um formulário eletrônico (como e-mail) para uma CA confiável para assinatura.

      Você deve manter uma cópia da chave privada e do certificado assinado pela CA para referência futura.

   Após processar sua solicitação, a CA envia o certificado digital assinado.

   a. Instale o certificado assinado pela CA usando o `security certificate install` comando com o `-type client` parâmetro.
   b. Digite o certificado e a chave privada quando você for solicitado e pressione **Enter**.
   c. Insira quaisquer certificados raiz ou intermediários adicionais quando for solicitado e pressione **Enter**.

      Você instala um certificado intermediário no cluster ou SVM se uma cadeia de certificados que começa na CA raiz confiável e termina com o certificado SSL emitido para você estiver faltando os certificados intermediários. Um certificado intermediário é um certificado subordinado emitido pela raiz confiável especificamente para emitir certificados de servidor de entidade final. O resultado é uma cadeia de certificados que começa na CA raiz confiável, passa pelo certificado intermediário e termina com o certificado SSL emitido para você.

3. Forneça o `client-ca` certificado do cluster ou SVM ao administrador do servidor SSL para instalação no servidor.

   O comando show do certificado de segurança com os `-instance` parâmetros e `-type client-ca` exibe as `client-ca` informações do certificado.

Instale um certificado de cliente assinado pela CA para o servidor KMIP

O subtipo de certificado do Key Management Interoperability Protocol (KMIP) (o parâmetro -subtype kmip-cert), juntamente com os tipos cliente e servidor-CA, especifica que o certificado é usado para autenticar mutuamente o cluster e um gerenciador de chaves externo, como um servidor KMIP.

Sobre esta tarefa

Instale um certificado KMIP para autenticar um servidor KMIP como um servidor SSL no cluster.

Passos

1. Use o `security certificate install` comando com os `-type server-ca` parâmetros e `-subtype kmip-cert` para instalar um certificado KMIP para o servidor KMIP.
2. Quando lhe for solicitado, introduza o certificado e, em seguida, prima Enter.

   O ONTAP lembra que você deve manter uma cópia do certificado para referência futura.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Controle de acesso baseado em atributos

Controle de acesso baseado em atributos com ONTAP

É possível implementar RBAC aprimorado com atributos e controle de acesso baseado em atributos (ABAC) usando o ONTAP. O ONTAP fornece várias abordagens que um cliente pode usar para obter ABAC no nível do arquivo, incluindo NFS 4,2 e XATTRS rotulados usando NFS e SMB/CIFS.

O controle de acesso baseado em atributos (ABAC) é um método sofisticado para gerenciar direitos de acesso que considera atributos do usuário, atributos de recursos e condições ambientais. O Instituto Nacional

de padrões e tecnologia (NIST) estabeleceu um padrão para a ABAC, fornecendo uma estrutura para sua implementação segura e consistente.

A partir do ONTAP 9.12,1, você pode configurar o ONTAP com rótulos de segurança NFSv4,2 e atributos estendidos (XATTRS) para que ele possa ser integrado a uma identidade de controle de acesso baseado em função (RBAC) e controle de acesso baseado em atributos (ABAC). Essa integração permite que o ONTAP acesse softwares de controle que são categorizados como uma solução de gerenciamento de dados compatível com ABAC NIST, oferecendo uma abordagem robusta e avançada para gerenciar direitos de acesso em ambientes complexos, incluindo ponto de aplicação de políticas (PEP), ponto de Decisão de políticas (PDP) e políticas que consideram atributos associados ao usuário, ao recurso e ao ambiente.

A integração do software NetApp ONTAP com atributos estendidos (XATTRS) e Controle de Acesso baseado em Atributo (ABAC) está alinhada com as diretrizes estabelecidas na publicação especial do NIST 800-162, garantindo o cumprimento das normas NIST para implementação da ABAC. O uso de rótulos de segurança NFS 4,2 e XATTRS permite a associação de atributos definidos pelo usuário com arquivos, atendendo aos requisitos do padrão NIST ABAC para considerar atributos de recursos nas decisões de controle de acesso. O PEP e PDP do software ABAC estão alinhados com o requisito do padrão NIST ABAC para esses componentes no processo de controle de acesso. A capacidade de definir políticas complexas que considerem vários atributos e condições alinha-se ao requisito do padrão NIST ABAC para controle de acesso baseado em políticas.

Informações relacionadas

- "Abordagens para ABAC com ONTAP"
- "NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"
- Pedido de comentários (RFC)
  - RFC 2203: Especificação do protocolo RPCSEC_GSS
  - RFC 3530: Protocolo NFS (Network File System) versão 4

Abordagens para ABAC com ONTAP

O ONTAP fornece abordagens variadas que um cliente pode usar para obter ABAC no nível do arquivo, incluindo NFSv4,2 e XATTRS rotulados usando NFS e SMB/CIFS.

Identificada como NFSv4,2

A partir do ONTAP 9.9,1, o recurso NFSv4,2 chamado NFS é suportado.

O NFS rotulado é uma maneira de gerenciar o acesso granular a arquivos e pastas usando rótulos SELinux e Controle de Acesso obrigatório (MAC). Esses rótulos MAC são armazenados com arquivos e pastas e funcionam em conjunto com permissões UNIX e ACLs NFSv4.x.

O suporte para NFS rotulado significa que a ONTAP agora reconhece e compreende as configurações de rótulo SELinux do cliente NFS. O NFS rotulado é coberto pela RFC-7204.

Os casos de uso do rotulado NFSv4,2 incluem o seguinte:

- MAC rotulagem de imagens de máquina virtual (VM)
- Classificação de segurança de dados para o setor público (segredo, segredo principal e outras classificações)
- Conformidade de segurança
- Linux sem disco

Ative o rótulo NFSv4,2

Você pode ativar ou desativar o NFS rotulado com a seguinte opção de privilégio avançado:

```
[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support
(privilege: advanced)
```

Este parâmetro é opcional e a predefinição é `disabled`.

Modos de aplicação para o rótulo NFSv4,2

A partir do ONTAP 9.9,1, o ONTAP suporta os seguintes modos de aplicação:

- **Modo de servidor limitado**: O ONTAP não pode impor as etiquetas, mas pode armazená-las e transmiti-las.

  A capacidade de alterar rótulos MAC também depende do cliente para impor.

- **Modo convidado**: Se o cliente não estiver identificado como NFS-Aware (v4,1 ou inferior), os rótulos MAC não serão transmitidos.

Atualmente, o ONTAP não suporta o modo completo (armazenamento e aplicação de etiquetas MAC).

Exemplo de configuração do rotulado NFSv4,2

A configuração de exemplo a seguir demonstra conceitos usando o Red Hat Enterprise Linux versão 9,3 (Plow).

O usuário `jrsmith`, criado com base nas credenciais de John R. Smith, tem o seguinte Privileges de conta:

- Nome de utilizador `jrsmith`
- Privileges `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Há duas funções: A conta de administrador que é um usuário privilegiado e usuário `jrsmith`, conforme descrito na seguinte tabela MLS Privileges:

Usuários	Função	Tipo	Níveis
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

Neste ambiente de exemplo, o usuário `jrsmith` tem acesso a arquivos nos níveis `s0 s3` de . Podemos aprimorar as classificações de segurança existentes, conforme descrito abaixo, para garantir que os administradores não tenham acesso a dados específicos do usuário.

- s0: dados de usuário do administrador de privilégios
- s0: dados não classificados

- s1: confidencial
- s2: dados secretos
- s3: dados secretos principais

Siga as políticas de segurança da sua organização

Exemplo de etiqueta de segurança NFSv4,2 com MCS

Além do MLS (Multi-Level Security), outro recurso chamado MCS (Multi-Category Security) permite definir categorias como projetos.

Etiqueta de segurança NFS	Valor
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Atributos estendidos (XATTRS)

A partir do ONTAP 9.12,1, o ONTAP suporta xattrs. Os xattrs permitem que os metadados sejam associados a arquivos e diretórios além do que é fornecido pelo sistema, como listas de controle de acesso (ACLs) ou atributos definidos pelo usuário.

Para implementar o xattrs, você pode usar `setfattr` e `getfattr` utilitários de linha de comando no Linux para gerenciar xattrs de objetos de sistema de arquivos. Essas ferramentas fornecem uma maneira poderosa de gerenciar metadados adicionais para arquivos e diretórios. Eles devem ser usados com cuidado, pois o uso inadequado pode levar a comportamentos inesperados ou problemas de segurança. Consulte sempre as `setfattr` páginas de manual e `getfattr` ou outra documentação fiável para obter instruções de utilização detalhadas.

Quando o xattrs está habilitado em um sistema de arquivos ONTAP, os usuários podem definir, modificar e recuperar atributos arbitrários em arquivos. Esses atributos podem ser usados para armazenar informações adicionais sobre o arquivo que não é capturado pelo conjunto padrão de atributos de arquivo, como informações de controle de acesso.

Requisitos para usar xattrs em ONTAP

- Red Hat Enterprise Linux 8,4 ou posterior
- Ubuntu 22,04 ou posterior
- Cada arquivo pode ter até 128 xattrs
- as chaves xattr estão limitadas a 255 bytes
- O tamanho combinado da chave ou do valor é de 1.729 bytes por xattr
- Diretórios e arquivos podem ter xattrs
- Para definir e recuperar xattrs `w`, ou bits de modo de gravação devem estar ativados para o usuário e grupo

Casos de uso para xattrs

Os xattrs são utilizados dentro do namespace do usuário e não carregam nenhum significado intrínseco para o próprio ONTAP. Em vez disso, suas aplicações práticas são determinadas e gerenciadas exclusivamente pelo aplicativo do lado do cliente que interage com o sistema de arquivos.

exemplos de casos de uso do xattr:

- Gravando o nome do aplicativo responsável pela criação de um arquivo.
- Manter uma referência à mensagem de e-mail a partir da qual um arquivo foi obtido.
- Estabelecendo uma estrutura de categorização para organizar objetos de arquivo.
- Rotular arquivos com o URL de sua fonte de download original.

Comandos para gerenciar xattrs

- `setfattr`: Define um atributo estendido de um arquivo ou diretório:

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Exemplo de comando:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr`: Recupera o valor de um atributo estendido específico ou lista todos os atributos estendidos de um arquivo ou diretório:

  Atributo específico:
  `getfattr -n <attribute_name> <file or directory name>`

  Todos os atributos:
  `getfattr <file or directory name>`

  Exemplo de comando:

  ```
  getfattr -n user.comment example.txt
  ```

xattr	Valor
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Permissões de usuário com ACE para atributos estendidos

Uma entrada de controle de acesso (ACE) é um componente dentro de uma lista de controle de acesso (ACL) que define os direitos de acesso ou permissões concedidos a um usuário individual ou a um grupo de usuários para um recurso específico, como um arquivo ou diretório. Cada ACE especifica o tipo de acesso permitido ou negado e está associado a um responsável de segurança específico (identidade de usuário ou grupo).

Tipo de ficheiro	Recuperar xattr	Definir xattrs
Ficheiro	R	A, W, T
Diretório	R	T

Explicação das permissões necessárias para o xattrs:

Retrieve xattr: As permissões necessárias para um usuário ler os atributos estendidos de um arquivo ou diretório. O "R" significa que a permissão de leitura é necessária. * Definir xattrs*: As permissões necessárias para modificar ou definir os atributos estendidos. "A", "W" e "T" representam diferentes exemplos de permissões, como anexar, escrever e uma permissão específica relacionada ao xattrs. **Files**: Os usuários precisam anexar, escrever e potencialmente uma permissão especial relacionada ao xattrs para definir atributos estendidos. **Diretórios**: Uma permissão específica "T" é necessária para definir atributos estendidos.

Suporte ao protocolo SMB/CIFS para xattrs

O suporte da ONTAP para o protocolo SMB/CIFS se estende ao tratamento abrangente de xattrs, que são parte integrante dos metadados de arquivos em ambientes Windows. Os atributos estendidos permitem que usuários e aplicativos armazenem informações adicionais além do conjunto padrão de atributos de arquivo, como detalhes do autor, descritores de segurança personalizados ou dados específicos do aplicativo. A implementação SMB/CIFS da ONTAP garante que esses xatrs sejam totalmente suportados, permitindo uma integração perfeita com serviços e aplicativos do Windows que dependem desses metadados para a funcionalidade e aplicação de políticas.

Quando os arquivos são acessados ou transferidos por compartilhamentos SMB/CIFS gerenciados pelo ONTAP, o sistema preserva a integridade dos xatrs, garantindo que todos os metadados sejam mantidos e permaneçam consistentes. Isso é particularmente importante para manter as configurações de segurança e para aplicativos que dependem do xattrs para configuração ou operação. O manuseio robusto de xatrs da ONTAP no contexto SMB/CIFS garante que o compartilhamento de arquivos entre diferentes plataformas e ambientes seja confiável e seguro, proporcionando aos usuários uma experiência perfeita e aos administradores a garantia de que as políticas de governança de dados são mantidas. Seja para colaboração, arquivamento de dados ou conformidade, a atenção da ONTAP aos xatrs em compartilhamentos SMB/CIFS representa seu compromisso com a excelência no gerenciamento de dados e interoperabilidade em ambientes de sistemas operacionais mistos.

Ponto de aplicação da política (PEP) e ponto de decisão da política (PDP) na ABAC

Em um sistema de controle de acesso baseado em atributos (ABAC), o ponto de aplicação de políticas (PEP) e o PDP (Policy Decision Point) desempenham papéis cruciais. O PEP é responsável pela aplicação de políticas de controle de acesso, enquanto o PDP toma a decisão de conceder ou negar acesso com base nas políticas.

No contexto do snippet de código Python fornecido, o próprio script atua como um PEP. Ele impõe a decisão de controle de acesso, quer concedendo acesso ao arquivo abrindo-o e lendo seu conteúdo ou negando acesso através da criação de um `PermissionError`.

O PDP, por outro lado, faria parte do sistema SELinux subjacente. Quando o script tenta abrir o arquivo com um contexto específico do SELinux, o sistema SELinux verifica suas políticas para decidir se deseja conceder ou negar acesso. Esta decisão é então aplicada pelo script.

Abaixo está um exemplo detalhado de como esse código funciona em um ambiente ABAC:

1. O script define o contexto SELinux para `jrsmith` contexto usando a `selinux.setcon()` função. Isso é equivalente a `jrsmith` tentar acessar o arquivo.
2. O script tenta abrir o arquivo. É aqui que o PEP entra em jogo.
3. O sistema SELinux verifica suas políticas para ver se `jrsmith` (ou mais especificamente, um usuário com `jrsmith` contexto SELinux) tem permissão para acessar o arquivo. Esta é a função do PDP.
4. Se `jrsmith` for permitido acessar o arquivo, o sistema SELinux permite que o script abra o arquivo e o

script leia e imprima o conteúdo do arquivo.

5. Se `jrsmith` não for permitido acessar o arquivo, o sistema SELinux impede que o script abra o arquivo e o script gera um `PermissionError`.
6. O script restaura o contexto original do SELinux para garantir que a alteração temporária do contexto não afete outras operações.

Usando Python, o código para obter o contexto é mostrado abaixo onde o caminho do arquivo variável é o documento que deve ser verificado:

```
#Get the current context

context = selinux.getfilecon(file_path)[1]
```

Clonagem de ONTAP e SnapMirror

As tecnologias de clonagem e SnapMirror da ONTAP foram projetadas para fornecer recursos de replicação e clonagem de dados eficientes e confiáveis, garantindo que todos os aspetos dos dados de arquivos, incluindo atributos estendidos (xattrs), sejam preservados e transferidos junto com o arquivo. Os xattrs são críticos, pois armazenam metadados adicionais associados a um arquivo, como rótulos de segurança, informações de controle de acesso e dados definidos pelo usuário, essenciais para manter o contexto e integridade do arquivo.

Quando um volume é clonado usando a tecnologia FlexClone da ONTAP, uma réplica gravável exata do volume é criada. Esse processo de clonagem é instantâneo e eficiente em espaço, e inclui todos os dados e metadados de arquivos, garantindo que os xatrs sejam totalmente replicados. Da mesma forma, o SnapMirror garante que os dados sejam espelhados para um sistema secundário com fidelidade total. Isso inclui xattrs, que são cruciais para aplicativos que dependem desses metadados para funcionar corretamente.

Ao incluir xatrs nas operações de clonagem e replicação, o NetApp ONTAP garante que todo o conjunto de dados, com todas as suas características, esteja disponível e consistente em sistemas de storage primário e secundário. Essa abordagem abrangente ao gerenciamento de dados é vital para organizações que exigem proteção de dados consistente, recuperação rápida e adesão a padrões regulatórios e de conformidade. Ele também simplifica o gerenciamento de dados em diferentes ambientes, seja no local ou na nuvem, fornecendo aos usuários a confiança de que seus dados estão completos e inalterados durante esses processos.

NFSv4,2 as etiquetas de segurança têm as ressalvas definidas no 2.

Exemplos de controle do acesso aos dados

A seguinte entrada de exemplo para dados armazenados no cert PKI de John R Smith mostra como a abordagem do NetApp pode ser aplicada a um arquivo e fornecer controle de acesso refinado.

Esses exemplos são para fins ilustrativos, e é responsabilidade do governo definir quais metadados são rótulos de segurança NFSv4,2 e xattrs. Detalhes sobre a atualização e retenção de rótulos são omitidos para simplificar.

Chave	Valor
EntitySecurityMark	t:S01 NÃO CLASSIFICADO

Chave	Valor

Informações	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

especificação	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganization	{
	"value": "DoD"
	}

Chave	Valor

briefings	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

CitizensaStatus	{
	"value": "US"
	}

folgas	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

CountryOfAffiliations	[
	{
	"value": "USA"
	}
	]

Chave	Valor

DigitalIdentifier	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

It is always	{
	"value": "DoD"
	}

DutyOrganization	{
	"value": "DoD"
	}

Tipo de entidade	{
	"value": "GOV"
	}

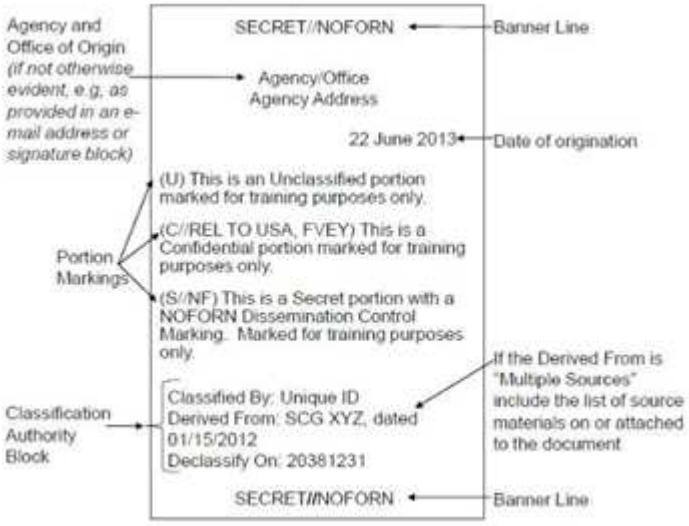
FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

Esses direitos PKI mostram os detalhes de acesso de John R. Smith, incluindo acesso por tipo de dados e atribuição.

Se John R. Smith criou e salvou um documento chamado *"sample_analysis.doc"*, de acordo com as questões relevantes de orientação política, o usuário adicionaria as marcas apropriadas de banner e porção, agência e escritório de origem e bloco de autoridade de classificação adequado com base na classificação do documento, conforme mostrado na imagem a seguir. Estes metadados ricos só são compreensíveis depois de

terem sido digitalizados pelo processamento de linguagem Natural (PNL) e terem regras aplicadas para fazer sentido a partir das marcações. Ferramentas como a classificação NetApp BlueXP podem fazer isso, mas são menos eficientes para decisões de controle de acesso, porque exigem permissão para olhar dentro do documento.

Marcação da parte do documento CAPCO não classificada



Em cenários em que os metadados IC-TDF são armazenados separadamente do arquivo, o NetApp defende uma camada adicional de controle de acesso refinado. Isso envolve o armazenamento de informações de controle de acesso tanto no nível de diretório quanto em associação com cada arquivo. Como exemplo, considere as seguintes tags vinculadas a um arquivo:

- NFSv4,2 rótulos de segurança: Utilizados para tomar decisões de segurança
- Xattrs: Fornecer informações complementares pertinentes ao arquivo e aos requisitos do programa organizacional

Os pares chave-valor a seguir são exemplos de metadados que podem ser armazenados como xattrs e oferecer informações detalhadas sobre o criador do arquivo e classificações de segurança associadas. Esses metadados podem ser aproveitados por aplicativos clientes para tomar decisões de acesso informado e organizar arquivos de acordo com os padrões e requisitos organizacionais.

Chave	Valor
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Chave	Valor

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Chave	Valor
user.geo_point	[-78.7941, 35.7956]

```
    }
}
```

Auditoria de alterações em rótulos

A auditoria de alterações em rótulos de segurança xattrs ou NFS é um aspeto crítico do gerenciamento e da segurança do sistema de arquivos. As ferramentas padrão de auditoria do sistema de arquivos permitem o monitoramento e o Registro de todas as alterações em um sistema de arquivos, incluindo modificações em atributos estendidos e rótulos de segurança.

Em ambientes Linux, o `auditd` daemon é comumente usado para estabelecer auditoria para eventos de sistema de arquivos. Ele permite que os administradores configurem regras para observar chamadas específicas do sistema relacionadas a alterações xattr, como `setxattr`, `lsetxattr` e `fsetxattr` para definir atributos e, `lremovexattr` e `fremovexattr` para `removexattr` remover atributos.

O ONTAP FPolicy amplia esses recursos fornecendo uma estrutura robusta para monitoramento e controle em tempo real de operações de arquivos. O FPolicy pode ser configurado para oferecer suporte a vários eventos xattr, oferecendo controle granular sobre as operações de arquivos e a capacidade de aplicar políticas abrangentes de gerenciamento de dados.

Para usuários que utilizam xattrs, especialmente em ambientes NFSv3 e NFSv4, apenas determinadas combinações de operações de arquivos e filtros são suportadas para monitoramento. A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 e NFSv4 é detalhada abaixo:

Operações de arquivos compatíveis	Filtros suportados
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory

Exemplo de um snippet de log auditd para uma operação setattr:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

Ativar o ONTAP FPolicy para usuários que trabalham com o xattrs fornece uma camada de visibilidade e controle essencial para manter a integridade e a segurança do sistema de arquivos. Ao aproveitar os recursos avançados de monitoramento da FPolicy, as organizações podem garantir que todas as alterações aos xattrs

sejam rastreadas, auditadas e alinhadas com seus padrões de segurança e conformidade. Essa abordagem proativa para o gerenciamento do sistema de arquivos é por isso que habilitar o ONTAP FPolicy é altamente recomendado para qualquer organização que queira aprimorar suas estratégias de governança e proteção de dados.

Integração com software de controle de acesso e identidade ABAC

Para aproveitar totalmente os recursos do controle de acesso baseado em atributos (ABAC), o ONTAP pode se integrar com um software de gerenciamento de identidade e acesso orientado para ABAC.

> Em paralelo a este conteúdo, o NetApp tem uma implementação de referência usando GreyBox. Uma suposição para este conteúdo é que os serviços de identidade, autenticação e acesso do governo incluem, no mínimo, um ponto de aplicação da Política (PEP) e um ponto de Decisão da Política (PDP) que atuam como intermediários para o acesso ao sistema de arquivos.

Em um ambiente prático, uma organização empregaria uma mistura de rótulos de segurança NFS e xattrs. Eles são usados para representar uma variedade de metadados, incluindo classificação, segurança, aplicativo e conteúdo, que são todos fundamentais para tomar decisões ABAC. O XATTR, por exemplo, pode ser usado para armazenar os atributos de recursos que o PDP usa para seu processo de tomada de decisão. Um atributo pode ser definido para representar o nível de classificação de um arquivo (por exemplo, "não classificado", "confidencial", "segredo" ou "segredo superior"). O PDP poderia então utilizar este atributo para impor uma política que restringe os utilizadores a aceder apenas a ficheiros que tenham um nível de classificação igual ou inferior ao nível de autorização.

Exemplo de fluxo de processo para ABAC

1. O usuário apresenta credenciais (por exemplo, PKI, OAuth, SAML) para acesso ao sistema ao PEP e obtém resultados do PDP.

   A função do PEP é intercetar a solicitação de acesso do usuário e encaminhá-la para o PDP.

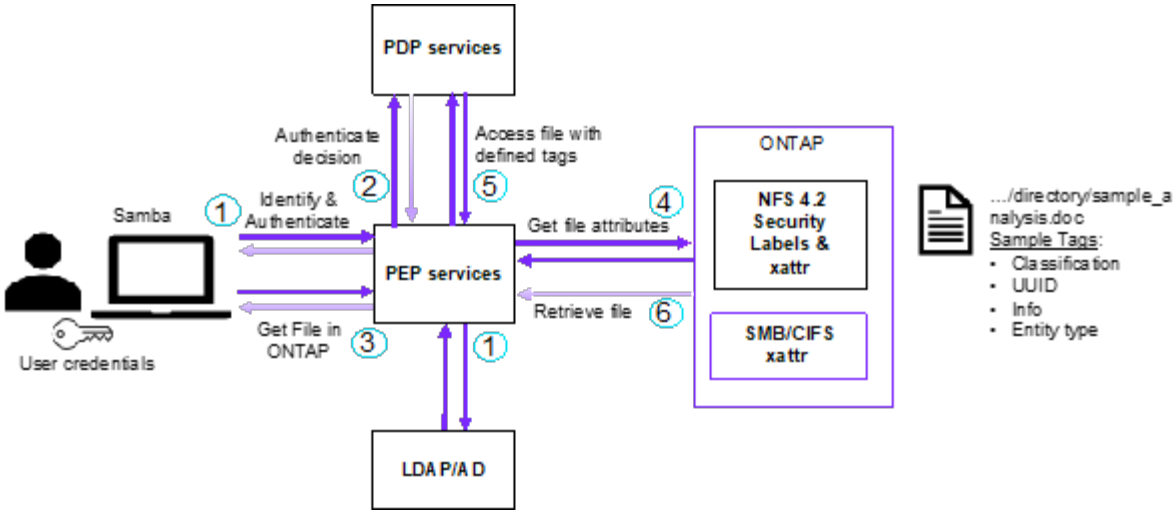
2. Em seguida, o PDP avalia essa solicitação em relação às políticas estabelecidas da ABAC.

   Essas políticas consideram vários atributos relacionados ao usuário, ao recurso em questão e ao ambiente circundante. Com base nessas políticas, o PDP toma uma decisão de acesso para permitir ou negar e, em seguida, comunica essa decisão de volta ao PEP.

   PDP fornece política para PEP para fazer cumprir. O PEP então impõe essa decisão, concedendo ou negando o pedido de acesso do usuário conforme decisão do PDP.

3. Após uma solicitação bem-sucedida, o usuário solicita um arquivo armazenado no ONTAP (AFF, AFF-C, por exemplo).
4. Se a solicitação for bem-sucedida, o PEP obtém tags de controle de acesso de grãos finos do documento.
5. PEP solicita política para o utilizador com base nos certificados desse utilizador.
6. O PEP toma uma decisão com base na política e nas tags se o usuário tiver acesso ao arquivo e permitir que o usuário recupere o arquivo.

> O acesso real pode ser feito usando tokens que não são protegidos.



Informações relacionadas

- "NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"
- Pedido de comentários (RFC)
  - RFC 2203: Especificação do protocolo RPCSEC_GSS
  - RFC 3530: Protocolo NFS (Network File System) versão 4

Segurança e criptografia de dados

Sobre a proteção contra ransomware da NetApp

Portfólio de proteção de ransomware e NetApp

O ransomware continua sendo uma das ameaças mais significativas que causam interrupções nos negócios na organização em 2024. De acordo com o "Sophos State of ransomware 2024", os ataques de ransomware afetaram 72% do público pesquisado. Os ataques de ransomware evoluíram para serem mais sofisticados e direcionados, com os agentes de ameaças empregando técnicas avançadas como inteligência artificial para maximizar seu impactos e lucros.

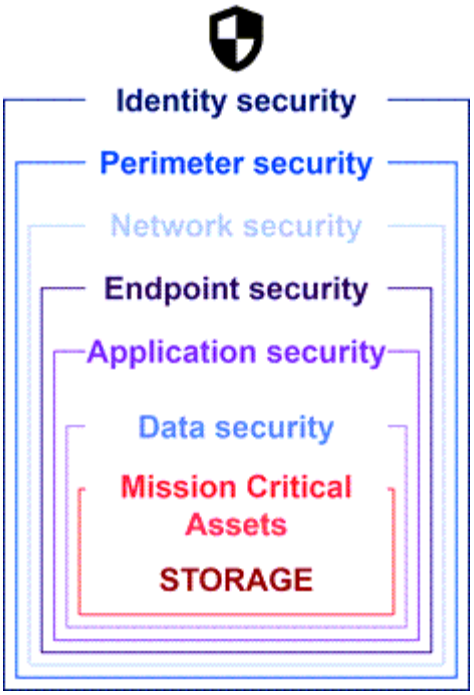
As organizações devem examinar toda a postura de segurança de perímetro, rede, identidade, aplicativo e onde os dados estão no nível de storage e proteger essas camadas. A adoção de uma abordagem centrada em dados à proteção cibernética na camada de storage é crucial no cenário de ameaças atual. Embora nenhuma solução única possa impedir todos os ataques, o uso de um portfólio de soluções, incluindo parcerias e terceiros, oferece uma defesa em camadas.

O Portfólio de produtos NetApp oferece várias ferramentas eficazes de visibilidade, detecção e correção, ajudando você a identificar ransomware com antecedência, prevenir propagação e se recuperar rapidamente, se necessário, para evitar tempo de inatividade caro. As soluções tradicionais de defesa em camadas continuam prevalecendo, assim como as soluções de terceiros e parceiros para visibilidade e detecção. A correção eficaz continua sendo uma parte crucial da resposta a qualquer ameaça. A abordagem exclusiva do setor que utiliza a tecnologia imutável Snapshot da NetApp e a solução SnapLock Logical AIR GAP é um diferencial do setor e a prática recomendada do setor para recursos de correção de ransomware.

> A partir de julho de 2024, o conteúdo do relatório técnico *TR-4572: NetApp ransomware Protection*, que foi publicado anteriormente como PDF, foi integrado ao restante da documentação do produto ONTAP.

Os dados são o alvo principal

Os cibercriminosos segmentam cada vez mais os dados diretamente, reconhecendo seu valor. Embora a segurança de perímetro, rede e aplicativos sejam importantes, eles podem ser ignorados. Com o foco na proteção de dados em sua origem, a camada de storage, fornece uma última linha de defesa crítica. Obter acesso aos dados de produção e criptografá-los ou torná-los inacessíveis é o objetivo dos ataques de ransomware. Para chegar lá, os invasores já devem ter perfurado as defesas existentes implantadas pelas organizações hoje, do perímetro à segurança do aplicativo.



Infelizmente, muitas organizações não aproveitam os recursos de segurança na camada de dados. É aqui que entra o portfólio de proteção contra ransomware da NetApp, protegendo você na última linha de defesa.

O custo real do ransomware

O pagamento de resgate em si não é o maior efeito monetário em um negócio. Embora o pagamento não seja insignificante, ele fica pálido em comparação com o custo do tempo de inatividade de sofrer um incidente de ransomware.

Os pagamentos de resgate são apenas um elemento dos custos de recuperação ao lidar com eventos de ransomware. Excluindo quaisquer resgates pagos, em 2024 as organizações relataram um custo médio para se recuperar de um ataque de ransomware de 2,73M dólares, um aumento de quase 1M dólares em relação aos 1,82M dólares relatados em 2023, de acordo com o "2024 Sophos State of ransomware" relatório. Para organizações que dependem muito da DISPONIBILIDADE DE TI, como e-commerce, negociação de ações e cuidados de saúde, os custos podem ser 10 vezes maiores ou mais.

Os custos do seguro cibernético também continuam a aumentar, dada a probabilidade muito real de um ataque de ransomware a empresas seguradas.

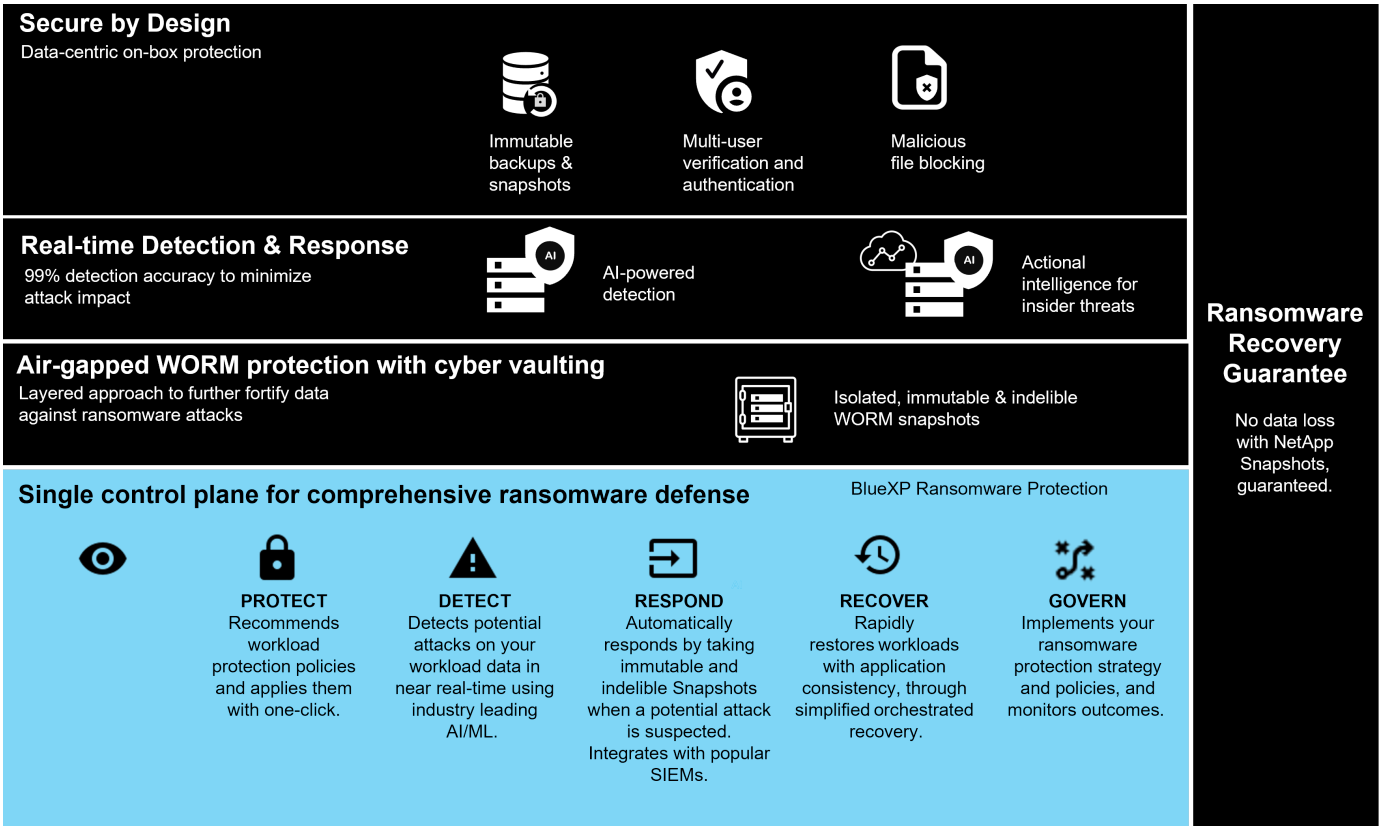
Proteção contra ransomware na camada de dados

A NetApp entende que sua postura de segurança é ampla e profunda em toda a organização, desde o perímetro até o local onde os dados estão na camada de storage. Sua pilha de segurança é complexa e deve fornecer segurança em todos os níveis de sua pilha de tecnologia.

A proteção em tempo real na camada de dados é ainda mais importante e tem requisitos exclusivos. Para serem eficazes, as soluções nessa camada devem oferecer esses atributos críticos:

- **Segurança por design** para minimizar a chance de ataque bem-sucedido
- **Detecção e resposta em tempo real** para minimizar o impactos de um ataque bem-sucedido
- **Proteção WORM com ar-gapped** para isolar backups de dados críticos
- * Um único plano de controle* para uma defesa abrangente contra ransomware

A NetApp pode oferecer tudo isso e muito mais.



Portfólio de proteção contra ransomware da NetApp

A NetApp "proteção incorporada contra ransomware"oferece defesa em tempo real, robusta e multifacetada para seus dados críticos. Na sua essência, os algoritmos avançados de detecção habilitados por IA monitoram continuamente os padrões de dados, identificando rapidamente possíveis ameaças de ransomware com precisão de 99%. Reagir rapidamente a ataques permite que nosso storage snapshots rapidamente os dados e proteja as cópias, garantindo uma recuperação rápida.

Para fortalecer ainda mais os dados, a capacidade do NetApp "vaulting cibernético"isola os dados com uma lacuna de ar lógica. Ao proteger os dados essenciais, garantimos a rápida continuidade dos negócios.

O NetApp "Proteção contra ransomware da BlueXP"reduz o sobrecarga operacional com um único plano de controle para coordenar e executar de forma inteligente uma defesa contra ransomware centrada no workload de ponta a ponta. Assim, você identifica e protege os dados críticos dos workloads em risco com um único clique. Com apenas um clique, a detecção e resposta precisas e automáticas para limitar o impacto de um possível ataque e recuperar workloads em minutos e não dias, protegendo os dados valiosos dos workloads e minimizando interrupções dispendiosos.

Como uma solução ONTAP nativa e integrada para proteger o acesso não autorizado aos seus dados, "Verificação multi-admin (MAV)" tem um conjunto robusto de recursos que garante que operações como excluir volumes, criar usuários administrativos adicionais ou excluir cópias snapshot possam ser executadas somente após aprovações de pelo menos um segundo administrador designado. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados. Você pode configurar quantos aprovadores de administrador designados desejar antes que uma cópia de snapshot possa ser excluída.

O NetApp ONTAP atende ao requisito para a autenticação de CLI SSH baseada na Web "Autenticação multifator (MFA)" no Gerenciador de sistema.

A proteção contra ransomware da NetApp oferece tranquilidade em um cenário de ameaças em constante evolução. Sua abordagem abrangente não só defende as variantes atuais de ransomware, mas também se adapta a ameaças emergentes, fornecendo segurança em longo prazo para sua infraestrutura de dados.

Saiba mais sobre outras opções de proteção

- "Proteção contra ransomware do Digital Advisor"
- "Segurança de carga de trabalho de armazenamento Cloud Insights (CISWS)"
- "FPolicy"
- "Cópias snapshot à prova de SnapLock e invioláveis"

Garantia de recuperação de ransomware

A NetApp oferece a garantia de restaurar os dados do Snapshot se ocorrer um ataque de ransomware. Nossa garantia: Se não pudermos ajudá-lo a restaurar seus dados de snapshot, faremos isso certo. A garantia está disponível em novas aquisições de sistemas AFF A-Series, AFF C-Series, ASA e FAS.

Saiba mais

- "Descrição do serviço de garantia de recuperação"
- "Blog de garantia de recuperação de ransomware".

Informações relacionadas

- "Página de recursos do site de suporte da NetApp"
- "Segurança do produto NetApp"

Cópias snapshot à prova de SnapLock e invioláveis para proteção de ransomware

Uma arma vital no arsenal de NetApp Snap é o SnapLock, que provou ser altamente eficaz na proteção contra ameaças de ransomware. Ao impedir a exclusão não autorizada de dados, o SnapLock fornece uma camada adicional de segurança, garantindo que os dados críticos permaneçam intactos e acessíveis, mesmo em caso de ataques mal-intencionados.

SnapLock Compliance

O SnapLock Compliance (SLC) fornece proteção indelével para seus dados. O SLC proíbe que os dados sejam excluídos mesmo quando um administrador tenta reinicializar a matriz. Ao contrário de outros produtos competitivos, o SnapLock Compliance não é vulnerável a ataques de engenharia social por meio das equipes de suporte desses produtos. Os dados protegidos por volumes do SnapLock Compliance são recuperáveis até que esses dados atinjam a data de expiração.

Para ativar o SnapLock, é necessária uma "ONTAP One" licença.

Saiba mais

- "Documentação do SnapLock"

Cópias Snapshot à prova de violações

As cópias Snapshot (TPS) à prova de violações fornecem uma maneira conveniente e rápida de proteger os dados de atos maliciosos. Ao contrário do SnapLock Compliance, o TPS é normalmente usado em sistemas primários onde o usuário pode proteger os dados por um determinado tempo e deixado localmente para recuperações rápidas ou onde os dados não precisam ser replicados fora do sistema primário. O TPS usa tecnologias SnapLock para impedir que a cópia snapshot principal seja excluída, mesmo por um administrador do ONTAP que use o mesmo período de expiração de retenção do SnapLock. A exclusão de cópias snapshot é impedida mesmo que o volume não esteja habilitado para SnapLock, embora os snapshots não tenham a mesma natureza indelével dos volumes SnapLock Compliance.

Para fazer cópias snapshot à prova de violações, é necessária uma "ONTAP One" licença.

Saiba mais

- "Bloqueie uma cópia snapshot para proteção contra ataques de ransomware".

Bloqueio de arquivos FPolicy

O FPolicy impede que arquivos indesejados sejam armazenados em seu dispositivo de armazenamento de nível empresarial. O FPolicy também oferece uma maneira de bloquear extensões de arquivo ransomware conhecidas. Um usuário ainda tem permissões de acesso total à pasta inicial, mas o FPolicy não permite que um usuário armazene arquivos que suas marcas de administrador como bloqueados. Não importa se esses arquivos são arquivos MP3 ou extensões de arquivo ransomware conhecidas.

Bloqueie arquivos maliciosos com o modo nativo FPolicy

O modo nativo do NetApp FPolicy (uma evolução do nome, Política de arquivos) é uma estrutura de bloqueio de extensão de arquivo que permite bloquear extensões de arquivo indesejadas de entrar em seu ambiente. Faz parte do ONTAP há mais de uma década e é incrivelmente útil para ajudar você a proteger contra ransomware. Esse mecanismo de confiança zero é valioso porque você obtém medidas de segurança extras além das permissões da lista de controle de acesso (ACL).

No ONTAP System Manager e no BlueXP , uma lista de mais de 3000 extensões de arquivo está disponível para referência.

> Algumas extensões podem ser legítimas em seu ambiente e bloqueá-las pode levar a problemas inesperados. Crie sua própria lista apropriada para o seu ambiente antes de configurar o FPolicy nativo.

O modo nativo FPolicy está incluído em todas as licenças do ONTAP.

Saiba mais

- "Blog: Fighting ransomware: Parte três - ONTAP FPolicy, outra ferramenta nativa poderosa (também conhecida como gratuita)"

Ative a análise de comportamento do usuário e da entidade (UEBA) com o modo externo FPolicy

O modo externo FPolicy é uma estrutura de notificação e controle de atividade de arquivo que fornece visibilidade da atividade de arquivo e do usuário. Essas notificações podem ser usadas por uma solução externa para executar análises baseadas em IA para detetar comportamentos maliciosos.

O modo externo FPolicy também pode ser configurado para aguardar a aprovação do servidor FPolicy antes de permitir que atividades específicas passem. Várias políticas como essa podem ser configuradas em um cluster, o que proporciona grande flexibilidade.

> Os servidores FPolicy devem ser responsivos às solicitações FPolicy se configurados para fornecer aprovação; caso contrário, o desempenho do sistema de storage pode ser afetado negativamente.

O modo externo FPolicy está incluído no "Todas as licenças ONTAP".

Saiba mais

- "Blog: Fighting ransomware: Parte quatro - UBA e ONTAP com o modo externo FPolicy."

Segurança de carga de trabalho de armazenamento Cloud Insights (CISWS)

A segurança de workload de storage (SWS) é um recurso do NetApp Cloud Insights que aprimora a postura de segurança, a capacidade de recuperação e a responsabilidade de um ambiente ONTAP. O SWS adota uma abordagem centrada no usuário, rastreando todas as atividades de arquivos de todos os usuários autenticados no ambiente. Ele usa análises avançadas para estabelecer padrões de acesso normais e sazonais para cada usuário. Esses padrões são usados para identificar rapidamente comportamentos suspeitos sem a necessidade de assinaturas de ransomware.

Quando o SWS deteta um potencial ransomware, exclusão de dados ou ataque de exfiltração, ele pode tomar ações automáticas, como:

- Tire um instantâneo do volume afetado.
- Bloqueie a conta de utilizador e o endereço IP suspeito de atividade maliciosa.
- Envie um alerta para administradores.

Como pode tomar medidas automatizadas para parar rapidamente uma ameaça privilegiada, bem como rastrear todas as atividades de arquivos, o SWS torna a recuperação de um evento de ransomware muito mais simples e rápida. Com ferramentas avançadas de auditoria e forense integradas, os usuários podem ver imediatamente quais volumes e arquivos foram afetados por um ataque, de qual conta de usuário o ataque veio e de que ação maliciosa foi realizada. Instantâneos automáticos mitigam os danos e aceleram a restauração de arquivos.

Alertas da proteção autônoma contra ransomware (ARP) da ONTAP também são visíveis no SWS, fornecendo uma única interface para clientes que usam ARP e SWS para proteger contra ataques de ransomware.

Saiba mais

- "NetApp Cloud Insights"

Detecção e resposta incorporadas baseada em IA on-box da NetApp ONTAP

À medida que as ameaças de ransomware se tornam cada vez mais sofisticadas, os seus mecanismos de defesa também devem ser aplicados. A proteção autônoma contra ransomware (ARP) da NetApp é baseada em AI com detecção inteligente de anomalias incorporada ao ONTAP. Ative-o para adicionar mais uma camada de defesa à sua resiliência cibernética.

ARP e ARP/AI são configuráveis por meio da interface de gerenciamento integrada do ONTAP, do Gerenciador de sistema e habilitados por volume.

Proteção autônoma contra ransomware (ARP)

A proteção autônoma contra ransomware (ARP), outra solução nativa da ONTAP incorporada desde 9.10.1, analisa a atividade do arquivo de workload de volume de storage nas e a entropia de dados para detectar automaticamente possíveis ransomwares. O ARP fornece aos administradores detecção, insights e um ponto de recuperação de dados em tempo real para deteção on-box de ransomware sem precedentes.

Para o ONTAP 9.15,1 e versões anteriores que suportam ARP, o ARP começa no modo de aprendizado para aprender a atividade típica de dados de carga de trabalho. Isso pode levar sete dias para a maioria dos ambientes. Depois que o modo de aprendizado estiver concluído, o ARP mudará automaticamente para o modo ativo e começará a procurar atividade anormal da carga de trabalho que possa potencialmente ser ransomware.

Se for detetada atividade anormal, uma cópia automática de instantâneos é imediatamente obtida, o que fornece um ponto de restauração o mais próximo possível do momento do ataque com dados infetados mínimos. Simultaneamente, é gerado um alerta automático (configurável) que permite que os administradores vejam a atividade anormal do arquivo para que possam determinar se a atividade é realmente maliciosa e tomar as medidas apropriadas.

Se a atividade for uma carga de trabalho esperada, os administradores podem marcá-la facilmente como um falso positivo. O ARP aprende essa mudança como atividade normal de carga de trabalho e não a sinaliza mais como um ataque potencial no futuro.

Para ativar o ARP, é necessária uma "ONTAP One" licença.

Saiba mais

- "Proteção autônoma contra ransomware"

Proteção autônoma contra ransomware/AI (ARP/AI)

Apresentado como uma prévia técnica no ONTAP 9.15,1, o ARP/AI leva a deteção em tempo real dos sistemas de armazenamento nas on-box para o próximo nível. A nova tecnologia de detecção habilitada por AI é treinada em mais de um milhão de arquivos e vários ataques de ransomware conhecidos. Além dos sinais usados no ARP, o ARP/AI também deteta criptografia de cabeçalho. A potência de IA e os sinais adicionais permitem que o ARP/AI forneça uma precisão de deteção superior a 99%. Isso foi validado pelo se Labs, um laboratório de testes independente que deu à ARP/AI a sua maior classificação AAA.

Como o treinamento dos modelos acontece continuamente na nuvem, o ARP/AI não requer um modo de aprendizado. Ele está ativo no momento em que é ligado. O treinamento contínuo também significa que o

ARP/AI sempre é validado contra novos tipos de ataque de ransomware à medida que eles surgem. O ARP/AI também vem com recursos de atualização automática que fornecem novos parâmetros a todos os clientes para manter a detecção de ransomware atualizada. Todos os outros recursos de deteção, insight e ponto de recuperação de dados do ARP são mantidos para ARP/AI.

Para ativar o ARP/AI, é necessária uma "ONTAP One" licença.

Saiba mais

- "Blog: A solução de deteção de ransomware em tempo real baseada em IA da NetApp atinge a classificação AAA"

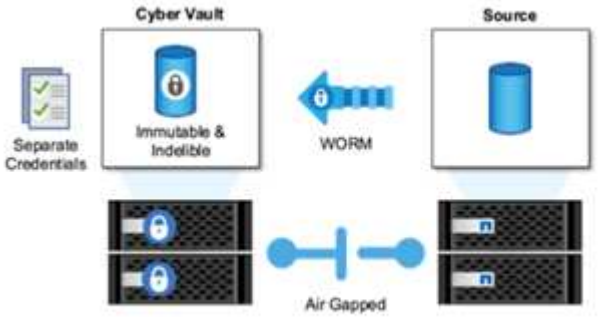
Proteção WORM com uso de cofres cibernéticos

A abordagem da NetApp a um cofre cibernético é uma arquitetura de referência criada especificamente para um cofre cibernético com conexão lógica. Essa abordagem aproveita as tecnologias de fortalecimento da segurança e conformidade, como o SnapLock, para permitir snapshots imutáveis e indeléveis.

Cyber vaulting com SnapLock Compliance e uma lacuna de ar lógica

Uma tendência crescente é que os invasores destruam as cópias de backup e, em alguns casos, até as criptografem. É por isso que muitos no setor de cibersegurança recomendam o uso de backups Air Gap como parte de uma estratégia geral de resiliência cibernética.

O problema é que as lacunas de ar tradicionais (fita e Mídia off-line) podem aumentar significativamente o tempo de restauração, aumentando assim o tempo de inatividade e os custos associados gerais. Mesmo uma abordagem mais moderna de uma solução de abertura de ar pode ser problemática. Por exemplo, se o cofre de backup for temporariamente aberto para receber novas cópias de backup e, em seguida, desconetar e fechar sua conexão de rede com dados primários para que mais uma vez sejam "trocados", um invasor pode aproveitar a abertura temporária. Durante o tempo em que a conexão está online, um invasor pode atacar para comprometer ou destruir os dados. Esse tipo de configuração geralmente também adiciona complexidade indesejada. Uma lacuna de ar lógica é um excelente substituto para uma lacuna de ar tradicional ou moderna, porque tem os mesmos princípios de proteção de segurança, mantendo o backup on-line. Com o NetApp, você pode resolver a complexidade do gapping de ar em fita ou disco com gapping lógico de ar, o que pode ser alcançado com cópias snapshot imutáveis e NetApp SnapLock Compliance.



A NetApp lançou o recurso SnapLock há mais de 10 anos para atender aos requisitos de conformidade de dados, como a Lei de portabilidade e responsabilidade de seguros de Saúde (HIPAA), a Sarbanes-Oxley e outras regras de dados regulatórios. Você também pode armazenar cópias snapshot primárias do SnapLock volumes para que as cópias possam ser comprometidas com WORM, impedindo a exclusão. Existem duas versões de licença SnapLock: SnapLock Compliance e SnapLock Enterprise. Para proteção contra ransomware, a NetApp recomenda o SnapLock Compliance porque você pode definir um período de retenção

específico durante o qual as cópias snapshot são bloqueadas e não podem ser excluídas, mesmo pelos administradores do ONTAP ou pelo suporte da NetApp.

Saiba mais

- "Blog: Visão geral do ONTAP Cyber Vault"

Cópias snapshot à prova de violações

Embora a utilização do SnapLock Compliance como uma lacuna lógica forneça a melhor proteção para impedir que atacantes excluam suas cópias de backup, ela exige que você mova as cópias snapshot usando o SnapVault para um volume secundário habilitado para SnapLock. Como resultado, muitos clientes implantam essa configuração em storage secundário na rede. Isso pode levar a tempos de restauração mais longos versus a restauração de uma cópia Snapshot de volume primário no storage primário.

A partir do ONTAP 9.12,1, as cópias snapshot à prova de violações fornecem proteção perto do nível SnapLock Compliance para suas cópias snapshot no storage primário e em volumes primários. Não há necessidade de armazenar a cópia Snapshot usando o SnapVault em um volume secundário SnapLocked. As cópias snapshot à prova de violações usam a tecnologia SnapLock para impedir que a cópia snapshot principal seja excluída, mesmo por um administrador completo da ONTAP usando o mesmo período de expiração de retenção da SnapLock. Isso possibilita tempos de restauração mais rápidos e o backup de um volume FlexClone por uma cópia Snapshot protegida e à prova de violações. Isso é algo que você não pode fazer com uma cópia Snapshot abobadada SnapLock Compliance tradicional.

A principal diferença entre as cópias snapshot da SnapLock Compliance e invioláveis é que o SnapLock Compliance não permite que o array ONTAP seja inicializado e apagado se existirem volumes SnapLock Compliance com cópias Snapshot abobadadas que ainda não atingiram sua data de expiração. Para fazer cópias Snapshot à prova de violações, é necessária uma licença SnapLock Compliance.

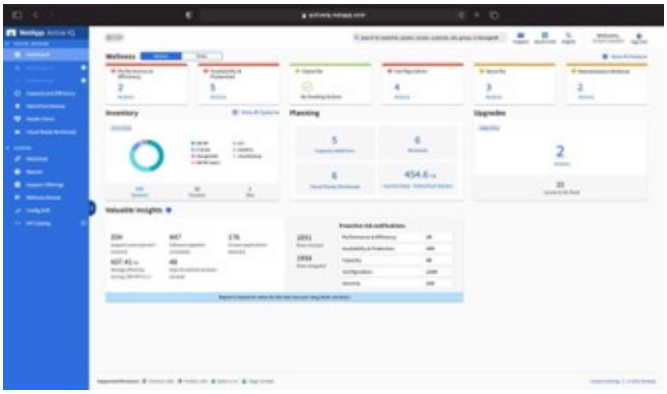
Saiba mais

- "Bloqueie uma cópia snapshot para proteção contra ataques de ransomware"

Proteção contra ransomware do Digital Advisor

O consultor digital da Active IQ (também conhecido como consultor digital) simplifica o cuidado proativo e a otimização do storage da NetApp com inteligência acionável para o gerenciamento ideal de dados. Alimentado por dados de telemetria de nossa base instalada altamente diversificada, ele usa técnicas avançadas de AI e ML para descobrir oportunidades de reduzir riscos e melhorar a performance e a eficiência do seu ambiente de storage.

Não só "Consultor digital da NetApp" pode ajudar "eliminar vulnerabilidades de segurança", mas também fornece insights e orientações específicos para a proteção contra ransomware. Um cartão de bem-estar dedicado mostra as ações necessárias e os riscos abordados, para que você possa ter certeza de que seus sistemas estão cumprindo essas recomendações de práticas recomendadas.



Os riscos e ações rastreados na página de bem-estar da Defesa do ransomware incluem o seguinte (e muito mais):

- A contagem de cópias snapshot de volume é baixa, diminuindo a possível proteção contra ransomware.
- O FPolicy não está habilitado para todas as máquinas virtuais de armazenamento (SVMs) configuradas para protocolos nas.

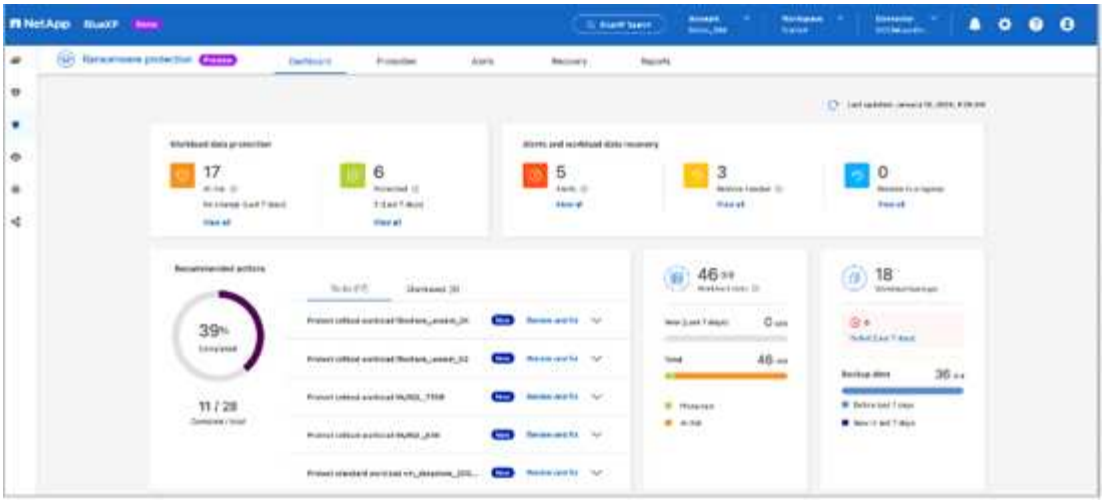
Para ver a proteção contra ransomware do Digital Advisor em ação, "Consultor digital da Active IQ"consulte .

Resiliência abrangente com proteção contra ransomware da BlueXP

É importante que a detecção de ransomware ocorra o mais cedo possível, para que você possa evitar a propagação e evitar tempo de inatividade caro. No entanto, uma estratégia eficaz de detecção de ransomware deve incluir mais do que uma única camada de proteção. A proteção contra ransomware da NetApp adota uma abordagem abrangente que inclui recursos on-box em tempo real, que se estendem a serviços de dados usando o BlueXP e uma solução isolada em camadas para cofres cibernéticos.

Proteção contra ransomware da BlueXP

O BlueXP é um único plano de controle para orquestrar, de forma inteligente, uma defesa abrangente e centrada em workload. A proteção contra ransomware do BlueXP reúne os recursos avançados de resiliência cibernética do ONTAP, como snapshots ARP, FPolicy e invioláveis, além de serviços de dados da BlueXP , como backup e recuperação do BlueXP . Ele também adiciona recomendações e orientações com fluxos de trabalho automatizados para fornecer uma defesa completa por meio de uma única IU. Ele opera no nível da carga de trabalho para garantir que os aplicativos que executam sua empresa sejam protegidos e possam ser recuperados o mais rápido possível em caso de ataque.



Benefícios para o cliente:

- A preparação assistida para ransomware reduz a sobrecarga operacional e melhora a eficácia
- A detecção de anomalias alimentada por IA/ML oferece maior precisão e resposta mais rápida para conter riscos
- A restauração orientada consistente com aplicações permite recuperar workloads com mais facilidade e em poucos minutos

"Proteção contra ransomware da BlueXP" Torna estas funções NIST mais fáceis de alcançar:

- **Descubra** e priorize dados automaticamente no armazenamento NetApp **com foco nas principais cargas de trabalho baseadas em aplicativos**.
- * Proteção com um clique* do backup de dados da carga de trabalho superior, configuração imutável e segura, bloqueio de arquivos maliciosos e domínio de segurança diferente.
- * Detecte com precisão* ransomware o mais rápido possível usando **detecção de anomalias baseada em IA de última geração.**
- Resposta automatizada e fluxos de trabalho e integração com as principais soluções **SIEM e XDR.**
- Restaure rapidamente os dados usando uma recuperação simplificada **orquestrada** para acelerar o tempo de atividade da aplicação.
- Implemente sua proteção contra ransomware * estratégia* e **políticas** e **monitore os resultados**.

Proteção autônoma contra ransomware

Saiba mais sobre a proteção autônoma contra ransomware no ONTAP

A partir do ONTAP 9.10,1, o recurso Autonomous ransomware Protection (ARP) usa análise de workload em ambientes nas (NFS e SMB) para detectar e avisar proativamente sobre atividades anormais que podem indicar um ataque. Quando um ataque é suspeito, o ARP também cria novos snapshots, além da proteção existente fornecida por snapshots programados.

Proteção autônoma contra ransomware com inteligência artificial (ARP/AI)

A partir do ONTAP 9.16,1, o ARP melhora a resiliência cibernética adotando um modelo de aprendizado de

máquina para análise anti-ransomware que deteta formas de ransomware em constante evolução com 99% de precisão. O modelo de aprendizado de máquina do ARP é pré-treinado em um grande conjunto de dados de arquivos antes e depois de um ataque simulado de ransomware. Esse treinamento intensivo em recursos é feito fora do ONTAP, mas o aprendizado desse treinamento é usado para o modelo dentro do ONTAP.

Transição imediata para o modo ativo para ARP/AI com volumes FlexVol

Com os volumes ARP/AI e FlexVol, não período de aprendizagemhá . O ARP/AI começa no modo ativo imediatamente após a instalação ou atualização para o 9,16. Depois de atualizar o cluster para o ONTAP 9.16,1, o ARP/AI será automaticamente ativado para volumes FlexVol existentes e novos se o ARP já estiver ativado para esses volumes.

"Saiba mais sobre como ativar o ARP/AI"

Atualizações automáticas ARP/AI

Para manter a proteção atualizada contra as ameaças mais recentes de ransomware, o ARP/AI oferece atualizações automáticas frequentes que ocorrem fora dos quadros regulares de atualização e liberação do ONTAP. Se tiver"atualizações automáticas ativadas", também poderá começar a receber atualizações automáticas de segurança para ARP/AI depois de selecionar atualizações automáticas para ficheiros de segurança. Você também pode optar por fazer essas atualizações manualmente e controlar quando as atualizações ocorrem.

A partir do ONTAP 9.16,1, as atualizações de segurança para ARP/AI estão disponíveis usando o Gerenciador do sistema, além das atualizações de sistema e firmware.

> ⓘ O recurso ARP/AI atualmente suporta apenas nas. Embora o recurso de atualização automática exiba a disponibilidade de novos arquivos de segurança para implantação no System Manager, essas atualizações são aplicáveis apenas à proteção da carga de trabalho nas.

"Saiba mais sobre as atualizações ARP/AI"

Licenças e capacitação

O suporte ARP está incluído no "Licença ONTAP ONE". Se você não tiver a licença ONTAP One, outras licenças estarão disponíveis para usar ARP que diferem dependendo da sua versão do ONTAP.

Lançamentos da ONTAP	Licença
ONTAP 9.11,1 e posterior	Anti_ransomware
ONTAP 9.10,1	MT_EK_MGMT (gerenciamento de chaves de vários clientes)

- Se você estiver atualizando do ONTAP 9.10,1 para o ONTAP 9.11,1 ou posterior e o ARP já estiver configurado em seu sistema, não será necessário instalar a nova licença Anti-ransomware. Para novas configurações ARP, a nova licença é necessária.
- Se você estiver revertendo do ONTAP 9.11,1 ou posterior para o ONTAP 9.10,1 e tiver ativado o ARP com a licença Anti-ransomware, verá uma mensagem de aviso e poderá precisar reconfigurar o ARP.

"Saiba mais sobre como reverter ARP".

Estratégia de proteção contra ransomware da ONTAP

Uma estratégia eficaz de detecção de ransomware deve incluir mais do que uma única camada de proteção.

Uma analogia seria as caraterísticas de segurança de um veículo. Você não confia em uma única caraterística, como um cinto de segurança, para protegê-lo completamente em um acidente. Os airbags, os travões antibloqueio e o aviso de colisão à frente são todos elementos de segurança adicionais que conduzirão a um resultado muito melhor. A proteção contra ransomware deve ser vista da mesma maneira.

Embora o ONTAP inclua recursos como FPolicy, snapshots, SnapLock e Active IQ Digital Advisor (também conhecido como consultor digital) para ajudar a proteger contra ransomware, as informações a seguir se concentram no recurso ARP on-box com recursos de aprendizado de máquina.

Para saber mais sobre outros recursos anti-ransomware do ONTAP, "Portfólio de proteção de ransomware e NetApp"consulte .

O que o ARP deteta

O ARP é projetado para proteger contra ataques de negação de serviço, onde o invasor retém dados até que um resgate seja pago. O ARP oferece detecção de ransomware em tempo real com base em:

- Identificação dos dados recebidos como encriptados ou em texto simples.
- Análises que detectam:
  - **Entropia**: Uma avaliação da aleatoriedade dos dados em um arquivo
  - **Tipos de extensão de arquivo**: Uma extensão que não está em conformidade com o tipo de extensão normal
  - **IOPS de arquivos**: Um aumento na atividade de volume anormal com criptografia de dados (a partir de ONTAP 9.11,1)

O ARP pode detetar a propagação da maioria dos ataques de ransomware depois que apenas um pequeno número de arquivos é criptografado, tomar medidas automaticamente para proteger os dados e alertá-lo de que um ataque suspeito está acontecendo.

> Nenhum sistema de prevenção ou detecção de ransomware pode garantir completamente a segurança de um ataque de ransomware. Embora seja possível que um ataque não seja detetado, o ARP atua como uma importante camada adicional de defesa se o software antivírus não conseguir detetar uma intrusão.

Aprendizagem e modos ativos

ARP tem dois modos:

- **Modo de aprendizagem** (ou modo "funcionamento a seco")
- **Modo ativo** (ou modo "ativado")

Modo de aprendizagem

Para todos os ARP em execução com ONTAP 9.10,1 a 9.15.1 e ARP usados para volumes FlexGroup com ONTAP 9.16,1, quando você ativa o ARP, ele é executado em *modo de aprendizagem*. No modo de aprendizagem, o sistema ONTAP desenvolve um perfil de alerta baseado nas áreas analíticas: Entropia, tipos de extensão de arquivo e IOPS de arquivos. Depois de executar o ARP no modo de aprendizado por tempo suficiente para avaliar as caraterísticas da carga de trabalho, você pode alternar para o modo ativo e começar a proteger seus dados.

Recomenda-se que você deixe o ARP no modo de aprendizado por 30 dias. A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo de aprendizagem ideal e automatiza o switch, que pode ocorrer antes de 30 dias.

O comando `security anti-ransomware volume workload-behavior show` mostra extensões de arquivo que foram detetadas no volume. Se você executar esse comando no início do modo de aprendizado e ele mostrar uma representação precisa dos tipos de arquivo, você não deve usar esses dados como base para mover para o modo ativo, já que o ONTAP ainda está coletando outras métricas.

Modo ativo

Para ARP em execução com ONTAP 9.10,1 a 9.15.1, o ARP muda para *ative mode* após o intervalo de aprendizagem ideal ser concluído. Com o ARP/AI a partir do ONTAP 9.16,1, não há período de aprendizado quando o ARP é usado com volumes FlexVol. O ARP/AI nos volumes FlexVol começa no modo ativo imediatamente após a instalação ou atualização para o 9.16.1. Se você estiver usando ONTAP 9.16,1 e ARP com volumes FlexGroup, um período de aprendizado ainda será necessário antes da transição para o modo ativo.

Depois que o ARP mudou para o modo ativo, o ONTAP cria instantâneos ARP para proteger os dados se uma ameaça for detetada.

No modo ativo, se uma extensão de arquivo for sinalizada como anormal, você deve avaliar o alerta. Você pode agir no alerta para proteger seus dados ou você pode marcar o alerta como um falso positivo. Marcar um alerta como falso positivo atualiza o perfil de alerta. Por exemplo, se o alerta for acionado por uma nova extensão de arquivo e você marcar o alerta como um falso positivo, você não receberá um alerta na próxima vez que essa extensão de arquivo for observada.

A partir de ONTAP 9.11,1, você pode personalizar os parâmetros de deteção para ARP. Para obter mais informações, Gerenciar parâmetros de deteção de ataque ARPconsulte .

Avaliação de ameaças e instantâneos ARP

No modo ativo, o ARP avalia a probabilidade de ameaça com base nos dados de entrada medidos em relação às análises aprendidas. Uma medição é atribuída quando o ARP deteta uma ameaça:

- **Low**: A deteção mais precoce de uma anomalia no volume (por exemplo, uma nova extensão de arquivo é observada no volume). Este nível de deteção só está disponível em versões anteriores ao ONTAP 9.16,1 que não têm ARP/AI.
- **Moderado**: Vários arquivos com a mesma extensão de arquivo nunca visto-antes são observados.
  - No ONTAP 9.10,1, o limite de escalonamento para moderar é de 100 ou mais arquivos.
  - Começando com ONTAP 9.11,1, a quantidade de arquivo é modificável; seu valor padrão é 20.

Em uma situação de baixa ameaça, o ONTAP deteta uma anormalidade e cria um instantâneo do volume para criar o melhor ponto de recuperação. O ONTAP prepende o nome do instantâneo ARP `Anti-ransomware-backup` para torná-lo facilmente identificável; por exemplo `Anti_ransomware_backup.2022-12-20_1248,.`

A ameaça aumenta para moderar depois que o ONTAP executa um relatório de análise determinando se a anormalidade corresponde a um perfil de ransomware. As ameaças que permanecem no nível baixo são registradas e visíveis na seção **Eventos** do System Manager. Quando a probabilidade de ataque é moderada, o ONTAP gera uma notificação EMS, solicitando que você avalie a ameaça. O ONTAP não envia alertas sobre baixas ameaças, no entanto, começando com ONTAP 9.14,1, você pode modificar definições de alertas. Para

obter mais informações, Responder a atividades anormaisconsulte .

Você pode visualizar informações sobre uma ameaça, independentemente do nível, na seção **Eventos** do System Manager ou com o `security anti-ransomware volume show` comando.

Instantâneos ARP individuais são retidos por dois dias. Se houver vários instantâneos ARP, eles serão retidos por cinco dias por padrão. A partir do ONTAP 9.11,1, você pode modificar as configurações de retenção. Para obter mais informações, Modificar opções para instantâneosconsulte .

Como recuperar dados no ONTAP após um ataque de ransomware

Quando um ataque é suspeito, o sistema obtém um instantâneo de volume nesse momento e bloqueia essa cópia. Se o ataque for confirmado mais tarde, o volume poderá ser restaurado usando o instantâneo ARP.

Os instantâneos bloqueados não podem ser eliminados por meios normais. No entanto, se você decidir mais tarde marcar o ataque como um falso positivo, a cópia bloqueada será excluída.

Com o conhecimento dos arquivos afetados e o tempo de ataque, é possível recuperar seletivamente os arquivos afetados de vários snapshots, em vez de simplesmente reverter todo o volume para um dos snapshots.

O ARP se baseia na comprovada tecnologia de recuperação de desastres e proteção de dados da ONTAP para responder a ataques de ransomware. Consulte os tópicos a seguir para obter mais informações sobre como recuperar dados.

- "Recuperar de instantâneos (System Manager)"
- "Restaurar arquivos de snapshots (CLI)"
- "Recuperação inteligente de ransomware"

Proteção de verificação multi-admin para ARP

A partir do ONTAP 9.13,1, é recomendável ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuário autenticados sejam necessários para a configuração ARP (Autonomous ransomware Protection). Para obter mais informações, "Ative a verificação de vários administradores"consulte .

Casos de uso e considerações da proteção autônoma contra ransomware

A proteção autônoma contra ransomware (ARP) está disponível para workloads nas a partir do ONTAP 9.10,1. Antes de implantar o ARP, você deve estar ciente dos usos recomendados e das configurações suportadas, bem como das implicações de desempenho.

Configurações suportadas e não suportadas

Ao decidir usar o ARP, é importante garantir que a carga de trabalho do seu volume seja adequada ao ARP e que atenda às configurações do sistema necessárias.

Workloads adequados

O ARP é adequado para:

- Bancos de dados no storage NFS

- Diretórios home do Windows ou do Linux

  Como os usuários podem criar arquivos com extensões que não foram detetadas no período de aprendizado, há maior possibilidade de falsos positivos nessa carga de trabalho.

- Imagens e vídeo

  Por exemplo, Registros de saúde e dados de automação de design eletrônico (EDA)

Cargas de trabalho inadequadas

O ARP não é adequado para:

- Cargas de trabalho com alta frequência de arquivos criam ou excluem (centenas de milhares de arquivos em poucos segundos; por exemplo, cargas de trabalho de teste/desenvolvimento).
- A deteção de ameaças do ARP depende de sua capacidade de reconhecer um aumento incomum na atividade de criação, renomeação ou exclusão de arquivos. Se o aplicativo em si for a origem da atividade do arquivo, ele não poderá ser distinguido efetivamente da atividade de ransomware.
- Cargas de trabalho em que o aplicativo ou o host criptografa dados. O ARP depende de distinguir os dados recebidos como criptografados ou não criptografados. Se o próprio aplicativo estiver criptografando os dados, a eficácia do recurso será reduzida. No entanto, o recurso ainda pode funcionar com base na atividade do arquivo (excluir, substituir ou criar, ou criar ou renomear com uma nova extensão de arquivo) e no tipo de arquivo.

Configurações compatíveis

O ARP está disponível para volumes NFS e SMB FlexVol em sistemas ONTAP locais a partir do ONTAP 9.10,1.

O suporte para outras configurações e tipos de volume está disponível nas seguintes versões do ONTAP:

	ONTAP 9.16,1	**ONTAP 9.15,1**	**ONTAP 9.14,1**	**ONTAP 9.13,1**	**ONTAP 9.12,1**	**ONTAP 9.11,1**	**ONTAP 9.10,1**
Volumes protegidos com o SnapMirror assíncrono	✓	✓	✓	✓	✓		
SVMs protegidas com SnapMirror assíncrono (recuperação de desastres da SVM)	✓	✓	✓	✓	✓		
Mobilidade de (`vserver migrate`dados SVM)	✓	✓	✓	✓	✓		

	ONTAP 9.16,1	ONTAP 9.15,1	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1	ONTAP 9.10,1
Volumes FlexGroup*	✓	✓	✓	✓			
Verificação multi-admin	✓	✓	✓	✓			
ARP/AI com atualizações automáticas	✓						

*ARP/AI não suporta volumes FlexGroup. Depois de ser atualizado para o ONTAP 9.16,1, os volumes FlexGroup habilitados para ARP continuam operando com o mesmo modelo ARP usado antes do ARP/AI.

Interoperabilidade SnapMirror e ARP

A partir do ONTAP 9.12,1, o ARP é suportado em volumes de destino assíncronos do SnapMirror. ARP não é ** suportado com SnapMirror síncrono.

Se um volume de origem do SnapMirror estiver habilitado para ARP, o volume de destino do SnapMirror adquirirá automaticamente o estado de configuração ARP (aprendizado, habilitado e assim por diante), os dados de treinamento ARP e o instantâneo criado pelo ARP do volume de origem. Nenhuma capacitação explícita é necessária.

Enquanto o volume de destino consiste em instantâneos somente leitura (RO), nenhum processamento ARP é feito em seus dados. No entanto, quando o volume de destino do SnapMirror é convertido para leitura-gravação (RW), o ARP é ativado automaticamente no volume de destino convertido em RW. O volume de destino não requer nenhum procedimento de aprendizagem adicional além do que já está gravado no volume de origem.

No ONTAP 9.10,1 e 9.11.1, o SnapMirror não transfere o estado de configuração ARP, os dados de treinamento e os snapshots dos volumes de origem para o destino. Assim, quando o volume de destino SnapMirror é convertido para RW, o ARP no volume de destino deve ser explicitamente ativado no modo de aprendizagem após a conversão.

ARP e máquinas virtuais

O ARP é compatível com máquinas virtuais (VMs). A deteção ARP comporta-se de forma diferente para alterações dentro e fora da VM. O ARP não é recomendado para cargas de trabalho com arquivos de alta entropia dentro da VM.

Alterações fora da VM

O ARP pode detetar alterações de extensão de arquivo em um volume NFS fora da VM se uma nova extensão entrar no volume criptografado ou uma extensão de arquivo mudar. As alterações de extensão de arquivo detetáveis são:

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .NVRAM

- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- - no.log

Alterações dentro da VM

Se o ataque de ransomware segmentar a VM e os arquivos dentro da VM são alterados sem fazer alterações fora da VM, o ARP deteta a ameaça se a entropia padrão da VM for baixa (por exemplo, arquivos .txt, .docx ou .mp4). Embora o ARP crie um snapshot de proteção nesse cenário, ele não gera um alerta de ameaça porque as extensões de arquivo fora da VM não foram adulteradas.

Se, por padrão, os arquivos forem de alta entropia (por exemplo, arquivos .gzip ou protegidos por senha), os recursos de deteção do ARP são limitados. O ARP ainda pode tirar instantâneos proativos nesta instância; no entanto, nenhum alerta será acionado se as extensões de arquivo não tiverem sido adulteradas externamente.

Configurações não suportadas

O ARP não é suportado nas seguintes configurações do sistema:

- Ambientes ONTAP S3
- AMBIENTES SAN

O ARP não suporta as seguintes configurações de volume:

- Volumes FlexGroup (em ONTAP 9.10,1 a 9.12.1. A partir do ONTAP 9.13,1, os volumes FlexGroup são suportados, mas são limitados ao modelo ARP usado antes do ARP/AI)
- Volumes FlexCache (ARP é suportado em volumes FlexVol de origem, mas não em volumes de cache)
- Volumes offline
- Volumes apenas de SAN
- Volumes SnapLock
- SnapMirror síncrono
- SnapMirror assíncrono (não suportado apenas no ONTAP 9.10,1 e 9.11.1. O SnapMirror Asynchronous é suportado a partir do ONTAP 9.12,1. Para obter mais informações, [snapmirror]consulte .)
- Volumes restritos
- Volumes raiz de VMs de storage
- Volumes de VMs de storage interrompidas

Considerações sobre desempenho e frequência ARP

O ARP pode ter um impactos mínimo no desempenho do sistema, conforme medido no throughput e IOPS de pico. O impactos do recurso ARP depende das cargas de trabalho de volume específicas. Para workloads comuns, os seguintes limites de configuração são recomendados:

Características do workload	Limite de volume recomendado por nó	Degradação do desempenho quando o limite de volume por nó é excedido, passa:[*]
Leitura intensiva ou os dados podem ser comprimidos.	150	4% do máximo de IOPS
Não é possível compactar dados com uso intensivo de gravação.	60	10% do máximo de IOPS

Pass:[*] o desempenho do sistema não é degradado além dessas porcentagens, independentemente do número de volumes adicionados além dos limites recomendados.

Como a análise ARP é executada em uma sequência priorizada, à medida que o número de volumes protegidos aumenta, a análise é executada em cada volume com menos frequência.

Verificação multi-admin com volumes protegidos com ARP

A partir do ONTAP 9.13,1, você pode ativar a verificação multi-admin (MAV) para segurança adicional com o ARP. O MAV garante que pelo menos dois ou mais administradores autenticados sejam necessários para desativar o ARP, pausar o ARP ou marcar um ataque suspeito como falso positivo em um volume protegido. Aprenda a "Ativar MAV para volumes protegidos por ARP".

Você precisa definir administradores para um grupo MAV e criar regras MAV para os `security anti-ransomware volume disable` comandos , `security anti-ransomware volume pause` e `security anti-ransomware volume attack clear-suspect` ARP que deseja proteger. Cada administrador no grupo MAV deve aprovar cada nova solicitação de regra e "Adicione a regra MAV novamente" dentro das configurações MAV.

A partir do ONTAP 9.14,1, o ARP oferece alertas para a criação de um instantâneo ARP e para a observação de uma nova extensão de arquivo. Os alertas para esses eventos são desativados por padrão. Os alertas podem ser definidos no volume ou no nível da SVM. Você pode criar regras MAV no nível SVM usando `security anti-ransomware vserver event-log modify` ou no nível de volume com `security anti-ransomware volume event-log modify`.

Próximas etapas

- "Ative a proteção Autonomous ransomware"
- "Ativar MAV para volumes protegidos por ARP"

Ative a proteção Autonomous ransomware

A partir do ONTAP 9.10,1, você pode ativar a proteção autônoma contra ransomware (ARP) em um volume existente ou criar um novo volume e ativar o ARP desde o início.

Se você quiser configurar o cluster do ONTAP para que todos os novos volumes sejam ativados por padrão para a proteção autônoma contra ransomware (ARP), consulte este "Procedimento ARP relacionado".

Sobre esta tarefa

- **Para ONTAP 9.10,1 a 9.15.1 e ARP com volumes FlexGroup** para essas versões do ONTAP, você deve sempre ativar o ARP inicialmente no "modo de aprendizagem"modo (ou "Dry-run"). Quando você ativa o ARP pela primeira vez no modo de aprendizado, o sistema analisa a carga de trabalho para caraterizar o comportamento normal. O início no modo ativo pode levar a relatórios falsos positivos excessivos.

Recomenda-se que o ARP seja executado no modo de aprendizagem por um mínimo de 30 dias. A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo ideal do período de aprendizagem e automatiza o switch, que pode ocorrer antes de 30 dias.

- **Para ONTAP 9.16,1 e posterior com volumes FlexVol** quando você ativa o ARP, a proteção ARP/AI começa imediatamente no modo ativo. Nenhum período de aprendizagem é necessário.

> Nos volumes existentes, os modos de aprendizagem e ativos aplicam-se apenas a dados recém-gravados, não a dados já existentes no volume. Os dados existentes não são digitalizados e analisados, porque as caraterísticas do tráfego de dados normal anterior são assumidas com base nos novos dados depois que o volume é ativado para ARP.

Antes de começar

- Você precisa ter uma VM de storage (SVM) habilitada para NFS, SMB (ou ambos).
- O licença correta tem de estar instalado para a versão do ONTAP.
- Você precisa ter um workload nas com clientes configurados.
- O volume em que deseja definir ARP deve estar protegido e ter um "caminho de junção"ativo .
- O volume tem de ser inferior a 100% cheio.
- É recomendável configurar o sistema EMS para enviar notificações por e-mail, que incluirão avisos de atividade ARP. Para obter mais informações, "Configurar eventos EMS para enviar notificações por e-mail"consulte .
- A partir do ONTAP 9.13,1, é recomendável ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuário autenticados sejam necessários para a configuração ARP (Autonomous ransomware Protection). Para obter mais informações, "Ative a verificação de vários administradores"consulte .

Ative ARP em um volume novo ou existente

Você pode ativar o ARP usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

Passos

1. Selecione **armazenamento > volumes** e, em seguida, selecione o volume que pretende proteger.
2. Na guia **Security** da visão geral **volumes**, selecione **Status** para alternar de Disabled (Desativado) para Enabled (habilitado).
   - Se você estiver usando ARP com ONTAP 9.15,1 ou anterior ou ONTAP 9.16,1 com volumes FlexGroup, selecione **Enabled in learning-mode** na caixa **Anti-ransomware**.

     A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo ideal do período de aprendizagem e automatiza o switch. "Desative essa configuração na VM de armazenamento associada"Pode controlar manualmente o modo de aprendizagem para a transição do modo ativo.

   - Se você estiver usando ARP em volumes FlexVol com ONTAP 9.16,1 ou posterior, a funcionalidade ARP/AI não requer um período de aprendizado e o modo ativo é selecionado por padrão.
3. Você pode verificar o estado ARP do volume na caixa **Anti-ransomware**.

   Para exibir o status ARP para todos os volumes: No painel **volumes**, selecione **Mostrar/Ocultar** e verifique se o status **Anti-ransomware** está marcado.

CLI

O processo para ativar o ARP com a CLI difere se você estiver habilitando-o em um volume existente versus um novo volume.

Ative ARP em um volume existente

1. Modifique um volume existente para habilitar a proteção contra ransomware:
   - Para ONTAP 9.15,1 e anterior e ARP com volumes FlexGroup, defina o estado do volume para `dry-run` (modo de aprendizagem):

     ```
     security anti-ransomware volume dry-run -volume <vol_name> -vserver
     <svm_name>
     ```

   - Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado do volume para `active` (modo ativo):

     ```
     security anti-ransomware volume active -volume <vol_name> -vserver
     <svm_name>
     ```

2. Se você atualizou para o ONTAP 9.13,1 ou posterior e o estado padrão ARP for `dry-run`, o aprendizado adaptável será ativado para que a alteração para o estado ativo seja feita automaticamente. Se você não quiser que esse comportamento seja ativado automaticamente, altere a configuração no nível SVM em todos os volumes associados:

   ```
   vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

3. Verifique o estado ARP do volume.

```
security anti-ransomware volume show
```

Ative ARP em um novo volume

1. Crie um novo volume com ARP ativado antes de provisionar dados:
   - Para ONTAP 9.15,1 e anterior e ARP com volumes FlexGroup, defina o estado para `dry-run` (modo de aprendizagem):

     ```
     volume create -volume <vol_name> -vserver <svm_name> -aggregate
     <aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
     </path_name>
     ```

   - Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado para `active` (modo ativo):

     ```
     volume create -volume <vol_name> -vserver <svm_name> -aggregate
     <aggr_name> -size <nn> -anti-ransomware-state active -junction-path
     </path_name>
     ```

2. Se você atualizou para o ONTAP 9.13,1 ou posterior e o estado padrão ARP for `dry-run`, o aprendizado adaptável será ativado para que a alteração para o estado ativo seja feita automaticamente. Se você não quiser que esse comportamento seja ativado automaticamente, altere a configuração no nível SVM em todos os volumes associados:

   ```
   vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

3. Verifique o estado ARP do volume.

   ```
   security anti-ransomware volume show
   ```

Informações relacionadas

- "Mude para o modo ativo após um período de aprendizagem"

Ative a proteção Autonomous ransomware por padrão em novos volumes

A partir do ONTAP 9.10,1, você pode configurar VMs de armazenamento (SVMs) para que novos volumes sejam ativados por padrão com a proteção Autônoma contra ransomware (ARP). Você pode modificar essa configuração usando o System Manager ou com a CLI.

Se você quiser configurar apenas volumes individuais novos ou existentes sem tornar o ARP o padrão, consulte este "Procedimento ARP relacionado".

Sobre esta tarefa

Por padrão, novos volumes são criados com ARP no modo desativado. O ARP só será ativado por padrão em novos volumes criados no SVM depois de ativar a funcionalidade ARP para volumes nas.

O ARP não será ativado automaticamente em volumes existentes. As alterações descritas neste procedimento afetam apenas novos volumes. Aprenda a "Ativar ARP para volumes existentes".

- **Para ONTAP 9.10,1 a 9.15.1 e ARP com volumes FlexGroup** por padrão, novos volumes habilitados com ARP ativado são definidos como "modo de aprendizagem"modo (ou "Dry-run") no qual o sistema analisa a carga de trabalho para caraterizar o comportamento normal. O modo de aprendizagem pode ser transferido para o modo ativo manualmente (todas as versões ARP) ou automaticamente (começando no ARP 9.13.1). Com o ARP 9.13.1 e posterior, o aprendizado adaptável foi adicionado à análise ARP para que a mudança do modo de aprendizado para o modo ativo seja feita automaticamente.
- **Para ONTAP 9.16,1 e posterior com volumes FlexVol** quando você ativa o ARP, a proteção ARP/AI começa imediatamente no modo ativo. Nenhum período de aprendizagem é necessário.

Antes de começar

- O licença correta tem de estar instalado para a versão do ONTAP.
- O volume tem de ser inferior a 100% cheio.
- Os caminhos de junção devem estar ativos.
- A partir do ONTAP 9.13,1, é recomendável ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuários autenticados sejam necessários para operações anti-ransomware. "Saiba mais".

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para ativar o ARP por padrão em novos volumes.

System Manager

1. Selecione **Storage > Storage VMs** e, em seguida, selecione a VM de armazenamento que contém volumes que você deseja proteger com ARP.
2. Navegue até a guia **Configurações**. Em **Segurança**, localize o bloco **Anti-ransomware** e selecione .
3. Marque a caixa para ativar o ARP para volumes nas. Marque a caixa adicional para ativar o ARP em todos os volumes nas elegíveis na VM de armazenamento.

   Para o ONTAP 9.16,1, o modo ativo é ativado automaticamente por padrão para novos volumes do FlexVol e nenhum período de aprendizado é necessário.

   Nos volumes existentes, os modos de aprendizagem e ativos aplicam-se apenas a dados recém-gravados, não a dados já existentes no volume. Os dados existentes não são digitalizados e analisados, porque as caraterísticas do tráfego de dados normal anterior são assumidas com base nos novos dados depois que o volume é ativado para ARP.

4. Se você atualizou para o ARP 9.13.1 ou posterior, opcionalmente selecione **alternar automaticamente do modo de aprendizado para o modo ativo após aprendizado suficiente**. Isso permite que o ARP determine o intervalo ideal do período de aprendizado e automatize o switch para o modo ativo.

CLI

- Modifique um SVM existente para ativar o ARP por padrão em novos volumes:
  - Para volumes ONTAP 9.15,1 e anteriores e FlexGroup, defina o estado predefinido para `dry-run` (modo de aprendizagem):

    ```
    vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state dry-run
    ```

  - Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado padrão para `active` (modo ativo):

    ```
    vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state active
    ```

- Crie um novo SVM com ARP habilitado por padrão para novos volumes:
  - Para volumes ONTAP 9.15,1 e anteriores e FlexGroup, defina o estado predefinido para `dry-run` (modo de aprendizagem):

    ```
    vserver create -vserver <svm_name> -anti-ransomware-default-volume-state dry-run <other parameters as needed>
    ```

  - Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado padrão para `active` (modo ativo):

    ```
    vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state active
    ```

- Se você atualizou para o ONTAP 9.13,1 ou posterior e o estado padrão for `dry-run`, o aprendizado adaptável será ativado para que a alteração para o estado ativo seja feita automaticamente. Modifique o SVM existente se você não quiser que esse comportamento seja ativado automaticamente:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

Informações relacionadas

- "Mude para o modo ativo após um período de aprendizagem"

Ative ARP/AI com a atualização automática

A partir do ONTAP 9.16,1, o ARP adotou a proteção autônoma contra ransomware com Inteligência artificial (ARP/AI) para melhorar a deteção e a resposta de ameaças. Depois de atualizar o cluster para o ONTAP 9.16,1, o ARP/AI será ativado automaticamente para volumes FlexVol se o ARP já estiver ativado para esses volumes. Se você não ativou o ARP ou não ativou as atualizações automáticas para o cluster, siga um dos cenários descritos neste procedimento.

Antes de atualizar para o ONTAP 9.16,1, "Feche todas as deteções ARP existentes".

Antes de começar

- Você deve ter volumes FlexVol para usar ARP/AI. Se você tiver volumes FlexGroup, o modelo ARP usado antes do ARP/AI continuará funcionando após a atualização para o ONTAP 9.16,1.

Quando você atualiza para o ONTAP 9.16,1, o ARP é ativado automaticamente no modo ativo para quaisquer instâncias ARP existentes com volumes FlexVol. Como o ARP/AI é treinado em um modelo extensivo de aprendizado de máquina, um período de aprendizado não é mais necessário. Quaisquer períodos de aprendizagem que não tenham sido concluídos antes da atualização serão automaticamente encerrados e os volumes serão transferidos para o modo ativo.

Passos

1. Siga o cenário específico da sua configuração:
   - *Para novos clusters executando o ONTAP 9.16,1*"Ativar ARP": . O ARP não está ativado por padrão. Depois de ativar o ARP, a funcionalidade ARP/AI é ativada automaticamente no modo ativo nos volumes que você escolher proteger.
   - **Para clusters existentes recentemente atualizados para ONTAP 9.16,1 que têm ARP ativado**: Nenhuma ação necessária. O ARP/AI se tornará automaticamente o novo método ARP de proteção contra ameaças nos volumes FlexVol que você escolheu proteger.
   - **Para clusters existentes recentemente atualizados para o ONTAP 9.16,1 que não tenham o ARP ativado**: "Ativar ARP". O ARP/AI se tornará automaticamente o novo método ARP de proteção contra ameaças depois de ativar o ARP.
2. Depois que o ARP/AI estiver ativado, decida se deseja que as atualizações de proteção ARP/AI sejam entregues e "automaticamente ou manualmente"instaladas.

Informações relacionadas

- "Atualizar ARP/AI"

Atualize a proteção Autonomous ransomware com AI (ARP/AI)

Para manter a proteção atualizada contra as ameaças mais recentes de ransomware, o ARP/AI oferece atualizações automáticas que ocorrem fora dos quadros regulares de liberação do ONTAP.

A partir do ONTAP 9.16,1, as atualizações de segurança para ARP/AI estão disponíveis em downloads de software do Gerenciador de sistema, além de atualizações de sistema e firmware. Se o cluster do ONTAP já estiver inscrito no "atualizações automáticas de sistema e firmware", você será notificado automaticamente quando as atualizações de segurança ARP/AI estiverem disponíveis. Você também pode alterar atualizar preferências para que o ONTAP instale as atualizações de segurança automaticamente.

Se desejar Atualizar manualmente ARP/AI, você pode baixar atualizações do site de suporte da NetApp e instalá-las usando o Gerenciador do sistema.

> O recurso ARP/AI atualmente suporta apenas nas. Embora o recurso de atualização automática exiba a disponibilidade de novos arquivos de segurança para implantação no System Manager, essas atualizações são aplicáveis apenas à proteção da carga de trabalho nas.

Sobre esta tarefa

Para o ONTAP 9.16,1 e posterior, você só pode atualizar o ARP/AI usando o Gerenciador do sistema.

Selecione uma preferência de atualização para ARP/AI

No System Manager, as definições na página Ativar atualizações automáticas para ficheiros de segurança são definidas como `Show notifications` se já estiver registado em atualizações automáticas de firmware e de sistema. Você pode alterar a configuração de atualização para `Automatically update` se preferir que o ONTAP aplique as atualizações mais recentes automaticamente. Se você usar um site escuro ou preferir executar atualizações manualmente, poderá optar por mostrar notificações ou ignorar automaticamente as atualizações de segurança.

Antes de começar

Para atualizações automáticas de segurança, "O AutoSupport e o AutoSupport OnDemand devem ser ativados e o protocolo de transporte deve ser definido como HTTPS".

Passos

1. No System Manager, clique em **Cluster > Settings > Software updates**.
2. Na seção **atualizações de software**, → selecione .
3. Na página **atualizações de software**, selecione a guia **todas as outras atualizações**.
4. Selecione a guia **todas as outras atualizações** e clique em **mais**.
5. Selecione **Editar definições de atualização automática**.
6. Na página Configurações de atualização automática, selecione **arquivos de segurança**.
7. Especifique a ação a ser tomada para arquivos de segurança (atualizações ARP/AI).

   Você pode optar por atualizar, mostrar notificações ou ignorar atualizações automaticamente.

Para que as atualizações de segurança sejam atualizadas automaticamente, o AutoSupport e o AutoSupport OnDemand devem ser ativados e o protocolo de transporte deve ser definido como HTTPS.

8. Aceite os termos e condições e selecione **Guardar**.

Atualize manualmente o ARP/AI com o pacote de segurança mais recente

Siga o procedimento apropriado, dependendo se você está registrado no Active IQ Unified Manager.

Certifique-se de instalar apenas uma atualização ARP mais recente do que a versão atual para evitar downgrades ARP não intencionais.

ONTAP 9.16,1 e posterior com Consultor Digital

Passos

1. No System Manager, vá para **Dashboard**.

   Na seção **Saúde**, uma mensagem será exibida se houver atualizações de segurança recomendadas para o cluster.

2. Clique na mensagem de alerta.
3. Ao lado das atualizações de segurança na lista de atualizações recomendadas, selecione **ações**.
4. Clique em **Atualizar** para instalar a atualização imediatamente ou **Agendar** para programá-la para mais tarde.

   Se a atualização já estiver agendada, você pode **Editar** ou **Cancelar**.

ONTAP 9.16,1 e posterior sem Consultor Digital

Passos

1. Navegue até "Site de suporte da NetApp"e inicie sessão.
2. Selecione o pacote de segurança que você deseja usar para atualizar seu cluster ARP/AI.
3. Copie os arquivos para um servidor HTTP ou FTP em sua rede ou para uma pasta local que pode ser acessada pelo cluster com ARP/AI.
4. No System Manager, clique em **Cluster > Settings > Software updates**.
5. Em **atualizações de software**, selecione a guia **todas as outras atualizações**.
6. No painel **atualizações manuais**, clique em **Adicionar arquivos de segurança** e adicione os arquivos usando uma destas preferências:
   - **Download do servidor**: Insira o URL do pacote de arquivos de segurança.
   - **Upload do cliente local**: Navegue até o arquivo TGZ baixado.

     Certifique-se de que o nome do ficheiro começa com `ontap_security_file_arpai_` e `.tgz` tem como uma extensão de ficheiro.

7. Clique em **Add** para aplicar as atualizações.

Verifique as atualizações ARP/AI

Para ver um histórico de atualizações automáticas que foram descartadas ou não foram instaladas, faça o seguinte:

1. No System Manager, clique em **Cluster > Settings > Software updates**.
2. Na seção **atualizações de software**, → selecione .
3. Na página **atualizações de software**, selecione a guia **todas as outras atualizações** e clique em **mais**.
4. Selecione **Ver todas as atualizações automáticas**.

Informações relacionadas

- "Ativar ARP/AI"
- "Assinaturas de e-mail para atualizações de software"

Mude para o modo ARP ativo após um período de aprendizagem

Para a proteção autônoma contra ransomware (ARP) 9.15.1 e anterior ou ARP em execução com volumes FlexGroup, alterne manualmente ou automaticamente um volume habilitado para ARP do modo de aprendizado para o modo ativo. Depois que o ARP tiver concluído uma execução de modo de aprendizagem de um mínimo recomendado de 30 dias, você pode alternar manualmente para o modo ativo. A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo ideal do período de aprendizagem e automatiza o switch, que pode ocorrer antes de 30 dias.

Se você estiver usando ARP em volumes FlexVol com ONTAP 9.16,1 ou posterior, a funcionalidade ARP/AI não requer um período de aprendizado e o modo ativo é selecionado por padrão.

> Nos volumes existentes, os modos de aprendizagem e ativos aplicam-se apenas a dados recém-gravados, não a dados já existentes no volume. Os dados existentes não são digitalizados e analisados, porque as caraterísticas do tráfego de dados normal anterior são assumidas com base nos novos dados depois que o volume é ativado para ARP.

Mude manualmente para o modo ativo após o período de aprendizagem

Para ONTAP 9.10,1 para 9.15.1 e ARP com volumes FlexGroup, você pode fazer a transição manualmente do modo de aprendizado ARP para o modo ativo usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

Passos

1. Selecione **armazenamento > volumes** e, em seguida, selecione o volume que está pronto para o modo ativo.
2. Na guia **Segurança** da visão geral **volumes**, selecione **mudar para o modo ativo** na caixa Anti-ransomware.
3. Você pode verificar o estado ARP do volume na caixa **Anti-ransomware**.

CLI

Passos

1. Quando o período de aprendizagem terminar, modifique o volume protegido para mudar para o modo ativo se ainda não tiver sido feito automaticamente:

   ```
   security anti-ransomware volume enable -volume <vol_name> -vserver
   <svm_name>
   ```

   Você também pode alternar para o modo ativo com o comando modificar volume:

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti-ransomware-state
   active
   ```

2. Verifique o estado ARP do volume.

   ```
   security anti-ransomware volume show
   ```

Mudança automática do modo de aprendizagem para o modo ativo

A partir do ONTAP 9.13,1, a aprendizagem adaptável foi adicionada à análise ARP e a mudança do modo de aprendizagem para o modo ativo é feita automaticamente. A decisão autônoma do ARP de alternar automaticamente do modo de aprendizado para o modo ativo é baseada nas configurações das seguintes opções:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

Após 30 dias de aprendizagem, um volume é automaticamente alterado para o modo ativo, mesmo que uma ou mais destas condições não estejam satisfeitas. Ou seja, se o interrutor automático estiver ativado, o volume muda para o modo ativo após um máximo de 30 dias. O valor máximo de 30 dias é fixo e não modificável.

Para obter mais informações sobre opções de configuração ARP, incluindo valores padrão, consulte "Referência do comando ONTAP".

Pausar a proteção Autonomous ransomware para excluir eventos de workload da análise

Se você está esperando eventos de carga de trabalho incomuns, você pode suspender e retomar temporariamente a análise ARP (Autonomous ransomware Protection) a qualquer momento.

A partir do ONTAP 9.13,1, você pode ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuário autenticados sejam necessários para pausar o ARP.

"Saiba mais sobre o MAV".

Sobre esta tarefa

Durante uma pausa ARP, nenhum evento é registrado nem nenhuma ação para novas gravações. No entanto, a operação de análise continua para logs anteriores em segundo plano.

> Não use a função de desativação ARP para pausar a análise. Isso desativa o ARP no volume e todas as informações existentes sobre o comportamento da carga de trabalho aprendida são perdidas. Isso exigiria um reinício do período de aprendizagem.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para pausar o ARP.

System Manager

1. Selecione **armazenamento > volumes** e, em seguida, selecione o volume em que deseja pausar ARP.
2. Na guia **Segurança** da visão geral dos volumes, selecione **Pausa anti-ransomware** na caixa **Anti-ransomware**.

> A partir do ONTAP 9.13,1, se você estiver usando MAV para proteger suas configurações ARP, a operação de pausa solicitará que você obtenha a aprovação de um ou mais administradores adicionais. "A aprovação deve ser recebida de todos os administradores" Associado ao grupo de aprovação MAV ou à operação falhará.

CLI

1. Pausar ARP em um volume:

   ```
   security anti-ransomware volume pause -vserver svm_name -volume vol_name
   ```

2. Para retomar o processamento, use o `resume` comando:

   ```
   security anti-ransomware volume resume -vserver svm_name -volume vol_name
   ```

3. Se você estiver usando MAV (disponível com ARP começando com ONTAP 9.13,1) para proteger suas configurações ARP, a operação de pausa solicitará que você obtenha a aprovação de um ou mais administradores adicionais. A aprovação deve ser recebida de todos os administradores associados ao grupo de aprovação MAV ou a operação falhará.

   Se você estiver usando MAV e uma operação de pausa esperada precisar de aprovações adicionais, cada aprovador de grupo MAV faz o seguinte:

   a. Mostrar o pedido:

      ```
      security multi-admin-verify request show
      ```

   b. Aprovar a solicitação:

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

      A resposta para o último aprovador de grupo indica que o volume foi modificado e o estado de ARP está pausado.

      Se você estiver usando MAV e for um aprovador de grupo MAV, poderá rejeitar uma solicitação de operação de pausa:

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Gerencie os parâmetros de deteção de ataque Autonomous ransomware Protection

A partir do ONTAP 9.11,1, você pode modificar os parâmetros para a deteção de ransomware em um volume específico com a proteção autônoma ativada e relatar um aumento conhecido como atividade de arquivo normal. Ajustar os parâmetros de deteção ajuda a melhorar a precisão dos relatórios com base na sua carga de trabalho de volume específica.

Como a deteção de ataque funciona

Quando o Autonomous ransomware Protection (ARP) está no modo de aprendizado, ele desenvolve valores de linha de base para comportamentos de volume. Estas são entropia, extensões de arquivo e, a partir de ONTAP 9.11,1, IOPS. Essas linhas de base são usadas para avaliar ameaças de ransomware. Para obter mais informações sobre esses critérios, O que o ARP detetaconsulte .

No ONTAP 9.10,1, o ARP emite um aviso se detetar ambas as seguintes condições:

- Mais de 20 arquivos com extensões de arquivo não observadas anteriormente no volume
- Dados de alta entropia

A partir do ONTAP 9.11,1, o ARP emite um aviso de ameaça se *somente* uma condição for atendida. Por exemplo, se mais de 20 arquivos com extensões de arquivo que não foram observadas anteriormente no volume forem observados dentro de um período de 24 horas, o ARP irá categorizar isso como uma ameaça *independentemente* da entropia observada. Os valores de 24 horas e 20 arquivos são padrões, que podem ser modificados.

> Para reduzir o número elevado de alertas falsos positivos, aceda a **armazenamento > volumes > Segurança > Configurar caraterísticas da carga de trabalho** e desative **Monitorizar novos tipos de ficheiros**. Esta configuração é desativada por padrão no ONTAP 9.14,1 P7, 9.15.1 P1 e 9.16.1 RC e posterior.

A partir do ONTAP 9.14,1, você pode configurar alertas quando o ARP observa uma nova extensão de arquivo e quando o ARP cria um snapshot. Para obter mais informações, [modify-alerts]consulte .

Certos volumes e workloads exigem parâmetros de detecção diferentes. Por exemplo, seu volume habilitado para ARP pode hospedar vários tipos de extensões de arquivo, caso em que você pode querer modificar a contagem de limite para extensões de arquivo nunca antes vistas para um número maior do que o padrão de 20 ou desativar avisos baseados em extensões de arquivo nunca antes vistas. A partir do ONTAP 9.11,1, você pode modificar os parâmetros de deteção de ataque para que eles se ajustem melhor às suas cargas de trabalho específicas.

Modificar parâmetros de deteção de ataque

Dependendo dos comportamentos esperados do seu volume habilitado para ARP, você pode querer modificar os parâmetros de deteção de ataque.

Passos

1. Veja os parâmetros de deteção de ataque existentes:

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                  Is Detection Based on File Create Rate? : true
                  Is Detection Based on File Rename Rate? : true
                  Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. Todos os campos mostrados são modificáveis com valores booleanos ou inteiros. Para modificar um campo, use o `security anti-ransomware volume attack-detection-parameters modify` comando.

   Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Relatar surtos conhecidos

O ARP continua a modificar os valores da linha de base para os parâmetros de deteção, mesmo no modo ativo. Se você souber de picos em sua atividade de volume, picos de uma vez ou um surto que é caraterístico de um novo normal, você deve denunciá-los como seguros. Relatar manualmente esses picos como seguros ajuda a melhorar a precisão das avaliações de ameaças da ARP.

Relatar um surto único

1. Se um surto único estiver ocorrendo em circunstâncias conhecidas e você quiser que o ARP relate um aumento semelhante em circunstâncias futuras, limpe o aumento do comportamento da carga de trabalho:

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   <svm_name> -volume <volume_name>
   ```

Modifique a oscilação da linha de base

1. Se um surto relatado deve ser considerado comportamento normal da aplicação, reporte o surto como tal para modificar o valor de oscilação da linha de base.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver <svm_name> -volume <volume_name>
   ```

Configurar alertas ARP

A partir do ONTAP 9.14,1, o ARP permite especificar alertas para dois eventos ARP:

- Observação de nova extensão de arquivo em um volume
- Criação de um instantâneo ARP

Os alertas desses dois eventos podem ser definidos em volumes individuais ou em toda a SVM. Se você ativar os alertas para o SVM, as configurações de alerta serão herdadas apenas por volumes criados após a ativação do alerta. Por padrão, os alertas não são ativados em nenhum volume.

Os alertas de eventos podem ser controlados com verificação multi-admin. Para obter mais informações, Verificação multi-admin com volumes protegidos com ARPconsulte .

System Manager

Definir alertas para um volume

1. Navegue até **volumes**. Selecione o volume individual para o qual pretende modificar as definições.
2. Selecione a guia **Segurança** e, em seguida, **Configurações de Segurança de Eventos**.
3. Para receber alertas para **Nova extensão de arquivo detetada** e **instantâneo ransomware criado**, selecione o menu suspenso sob o título **gravidade**. Modifique a configuração de **não gerar evento** para **Aviso**.
4. Selecione **Guardar**.

Definir alertas para um SVM

1. Navegue até **Storage VM** e selecione o SVM para o qual você deseja ativar as configurações.
2. Sob o título **Segurança**, localize o cartão **Anti-ransomware**. Selecione ⋮, em seguida, **Editar gravidade do evento ransomware**.
3. Para receber alertas para **Nova extensão de arquivo detetada** e **instantâneo ransomware criado**, selecione o menu suspenso sob o título **gravidade**. Modifique a configuração de **não gerar evento** para **Aviso**.
4. Selecione **Guardar**.

CLI

Definir alertas para um volume

- Para definir alertas para uma nova extensão de arquivo:

```
security anti-ransomware volume event-log modify -vserver <svm_name> -is
-enabled-on-new-file-extension-seen true
```

- Para definir alertas para a criação de um instantâneo ARP:

```
security anti-ransomware volume event-log modify -vserver <svm_name> -is
-enabled-on-snapshot-copy-creation true
```

- Confirme suas configurações com o `anti-ransomware volume event-log show` comando.

Definir alertas para um SVM

- Para definir alertas para uma nova extensão de arquivo:

```
security anti-ransomware vserver event-log modify -vserver <svm_name> -is
-enabled-on-new-file-extension-seen true
```

- Para definir alertas para a criação de um instantâneo ARP:

```
security anti-ransomware vserver event-log modify -vserver <svm_name> -is
-enabled-on-snapshot-copy-creation true
```

- Confirme suas configurações com o `security anti-ransomware vserver event-log show` comando.

Informações relacionadas

- "Entenda os ataques Autonomous ransomware Protection e o snapshot Autonomous ransomware Protection".

Responder a atividades anormais

Quando o Autonomous ransomware Protection (ARP) deteta atividade anormal em um volume protegido, ele emite um aviso. Você deve avaliar a notificação para determinar se a atividade é aceitável (falso positivo) ou se um ataque parece mal-intencionado.

Sobre esta tarefa

ARP exibe uma lista de arquivos suspeitos quando deteta qualquer combinação de alta entropia de dados, atividade de volume anormal com criptografia de dados e extensões de arquivos incomuns.

Quando o aviso for emitido, responda designando a atividade do ficheiro de duas formas:

- **Falso positivo**

  O tipo de arquivo identificado é esperado em sua carga de trabalho e pode ser ignorado.

- **Possível ataque de ransomware**

  O tipo de arquivo identificado é inesperado em sua carga de trabalho e deve ser Tratado como um potencial ataque.

Em ambos os casos, a monitorização normal é retomada após a atualização e limpeza dos avisos. O ARP Registra sua avaliação no perfil de avaliação de ameaças, usando sua escolha para monitorar atividades subsequentes de arquivos.

No caso de um ataque suspeito, você deve determinar se é um ataque, responder a ele, se for, e restaurar dados protegidos antes de limpar os avisos. "Saiba mais sobre como se recuperar de um ataque de ransomware".

Se você restaurar um volume inteiro, não há avisos para limpar.

Antes de começar

O ARP deve estar em execução no modo ativo.

Passos

Você pode usar o Gerenciador de sistema ou a CLI do ONTAP para responder a uma tarefa anormal.

System Manager

1. Quando receber uma notificação de "atividade anormal", siga o link. Alternativamente, navegue até a guia **Security** da visão geral **volumes**.

   Os avisos são exibidos no painel **Visão geral** do menu **Eventos**.

2. Quando for apresentada uma mensagem "Detected abnormal volume activity" (atividade de volume anormal detetada), visualize os ficheiros suspeitos.

   Na guia **Segurança**, selecione **Exibir tipos de arquivo suspeitos**.

3. Na caixa de diálogo **tipos de arquivo suspeitos**, examine cada tipo de arquivo e marque-o como "Falso positivo" ou "ataque de potencial ransomware".

Se selecionou este valor…	Tome esta ação…
Falso positivo	Selecione **Update** e **Clear Suspect File Types** para gravar sua decisão e retomar o monitoramento ARP normal. A partir do ONTAP 9.13,1, se você estiver usando o MAV para proteger suas configurações ARP, a operação clara suspeita solicitará que você obtenha a aprovação de um ou mais administradores adicionais. "A aprovação deve ser recebida de todos os administradores" Associado ao grupo de aprovação MAV ou à operação falhará.
Potencial ataque de ransomware	Responda ao ataque e restaure os dados protegidos. Em seguida, selecione **Update** e **Clear Suspect File Types** para gravar sua decisão e retomar o monitoramento ARP normal. Não há tipos de arquivo suspeitos para limpar se você restaurou um volume inteiro.

CLI

1. Quando receber uma notificação de um ataque de ransomware suspeito, verifique a hora e a gravidade do ataque:

   `security anti-ransomware volume show -vserver` *`svm_name`* `-volume` *`vol_name`*

   Saída da amostra:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

   Você também pode verificar mensagens EMS:

```
event log show -message-name callhome.arw.activity.seen
```

2. Gere um relatório de ataque e anote o local de saída:

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   Saída da amostra:

   ```
   Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
   "vs0:vol1/"
   ```

3. Exibir o relatório em um sistema de cliente admin. Por exemplo:

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. Execute uma das seguintes ações com base na avaliação das extensões de arquivo:

   - Falso positivo

     Digite o seguinte comando para Registrar sua decisão, adicionando a nova extensão à lista dos permitidos, e retomar o monitoramento normal anti-ransomware:
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     Use um dos seguintes parâmetros para identificar as extensões:
     `[-seq-no integer]` Número de sequência do arquivo na lista suspeita.
     `[-extension text, … ]` Extensões de arquivo
     `[-start-time date_time -end-time date_time]` começando e terminando tempos para o intervalo de arquivos a ser limpo, no formulário "MM/DD/AAAA HH:MM:SS".

   - Possível ataque de ransomware

     Responder ao ataque e "Recupere dados do instantâneo de backup criado pelo ARP". Depois que os dados forem recuperados, digite o seguinte comando para Registrar sua decisão e retomar o monitoramento ARP normal:

     ```
     anti-ransomware volume attack clear-suspect -vserver svm_name -volume
     vol_name [extension identifiers] -false-positive false
     ```

     Use um dos seguintes parâmetros para identificar as extensões:
     `[-seq-no integer]` Número de sequência do arquivo na lista suspeita
     `[-extension text, … ]` extensão de arquivo
     `[-start-time date_time -end-time date_time]` horários de início e término para o intervalo de arquivos a ser limpo, no formulário "MM/DD/AAAA HH:MM:SS".

Não há tipos de arquivo suspeitos para limpar se você restaurou um volume inteiro. O instantâneo de backup criado pelo ARP será removido e o relatório de ataque será limpo.

5. Se você estiver usando MAV e uma operação esperada `clear-suspect` precisar de aprovações adicionais, cada aprovador de grupo MAV deve:

   a. Mostrar o pedido:

      `security multi-admin-verify request show`

   b. Aprovar a solicitação para retomar o monitoramento normal anti-ransomware:

      `security multi-admin-verify request approve -index[`*`number returned from show request`*`]`

   A resposta para o último aprovador do grupo indica que o volume foi modificado e um falso positivo é registrado.

6. Se você estiver usando MAV e for um aprovador de grupo MAV, também poderá rejeitar uma solicitação clara e suspeita:

   `security multi-admin-verify request veto -index[`*`number returned from show request`*`]`

Mais informações

- "KB: Entendendo os ataques Autonomous ransomware Protection e o snapshot Autonomous ransomware Protection".

Restaure os dados após um ataque de ransomware

O Autonomous ransomware Protection (ARP) cria snapshots nomeados `Anti_ransomware_backup` quando deteta uma potencial ameaça de ransomware. Você pode usar um desses snapshots ARP ou outro snapshot do volume para restaurar dados.

Sobre esta tarefa

Se o volume tiver relações SnapMirror, replique manualmente todas as cópias espelhadas do volume imediatamente após a restauração a partir de um snapshot. Não fazer isso pode resultar em cópias espelhadas inutilizáveis que devem ser excluídas e recriadas.

Para restaurar a partir de um instantâneo diferente do `Anti_ransomware_backup` instantâneo após um ataque do sistema ter sido identificado, primeiro você deve liberar o instantâneo ARP.

Se nenhum ataque do sistema foi relatado, você deve primeiro restaurar a partir do `Anti_ransomware_backup` instantâneo e, em seguida, concluir uma restauração subsequente do volume a partir do instantâneo de sua escolha.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para restaurar seus dados.

System Manager

Restaurar após um ataque ao sistema

1. Para restaurar a partir do instantâneo ARP, passe para a etapa dois. Para restaurar a partir de um instantâneo anterior, primeiro é necessário liberar o bloqueio no instantâneo ARP.
   a. Selecione **armazenamento > volumes**.
   b. Selecione **Segurança** e depois **Exibir tipos de arquivos suspeitos**.
   c. Marque os arquivos como "possível ataque de ransomware".
   d. Selecione **Update** e **Clear Suspect File Types**.
2. Exibir os instantâneos em volumes:

   Selecione **armazenamento > volumes** e, em seguida, selecione o volume e **cópias Snapshot**.
3. Selecione ⋮ ao lado do instantâneo que deseja restaurar e depois **Restaurar**.

Restaure se um ataque do sistema não foi identificado

1. Exibir os instantâneos em volumes:

   Selecione **armazenamento > volumes** e, em seguida, selecione o volume e **cópias Snapshot**.
2. Selecione ⋮-os escolha o `Anti_ransomware_backup` instantâneo.
3. Selecione **Restaurar**.
4. Retorne ao menu **cópias instantâneas** e escolha o instantâneo que deseja usar. Selecione **Restaurar**.

CLI

Restaurar após um ataque ao sistema

1. Para restaurar a partir do instantâneo ARP, passe para a etapa dois. Para restaurar dados de instantâneos anteriores, você deve liberar o bloqueio no instantâneo ARP.

   ⓘ Só é necessário liberar o SnapLock anti-ransomware antes de restaurar a partir de snapshots anteriores se você estiver usando o `volume snap restore` comando como descrito abaixo. Se você estiver restaurando dados usando o FlexClone, a Restauração Snap de Arquivo único ou outros métodos, isso não será necessário.

   Marque o ataque como um possível ataque de ransomware (`-false-positive false`) e limpe os arquivos suspeitos (`clear-suspect`):
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive false` Use um dos seguintes parâmetros para identificar as extensões:
   `[-seq-no` *`integer`*`]` Número de sequência do arquivo na lista suspeita.
   `[-extension` *`text`*`, … ]` Extensões de arquivo
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` começando e terminando tempos para o intervalo de arquivos a ser limpo, no formulário "MM/DD/AAAA HH:MM:SS".
2. Listar as cópias Snapshot em um volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra as cópias Snapshot `vol1` no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Restaure o conteúdo de um volume a partir de uma cópia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

O exemplo a seguir restaura o conteúdo `vol1` de :

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Restaure se um ataque do sistema não foi identificado

1. Listar as cópias Snapshot em um volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra as cópias Snapshot `vol1` no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure o conteúdo de um volume a partir de uma cópia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

O exemplo a seguir restaura o conteúdo `vol1` de :

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

3. Repita as etapas 1 e 2 para restaurar o volume usando o instantâneo de desejo.

Informações relacionadas

- "KB: Prevenção e recuperação de ransomware no ONTAP"

Modificar opções para instantâneos automáticos

A partir do ONTAP 9.11,1, você pode usar a CLI para controlar as configurações de retenção de snapshots ARP (Autonomous ransomware Protection) que são gerados automaticamente em resposta a ataques suspeitos de ransomware.

Antes de começar

Você só pode modificar as opções de instantâneos ARP em um nó SVM.

Passos

1. Para mostrar todas as definições atuais de instantâneos ARP, introduza:
`vserver options -vserver <svm_name> -option-name arw*`

O `vserver options` comando é um comando oculto. Para visualizar a página de manual, entre `man vserver options` na CLI do ONTAP.

2. Para mostrar as definições atuais de instantâneos ARP selecionadas, introduza:
`vserver options -vserver <svm_name> -option-name <arw_setting_name>`
3. Para modificar as definições de instantâneos ARP, introduza:
`vserver options -vserver <svm_name> -option-name <arw_setting_name> -option -value <arw_setting_value>`

   As seguintes configurações são modificáveis:

Definição ARW	Descrição
`arw.snap.max.count`	Especifica o número máximo de instantâneos ARP que podem existir em um volume a qualquer momento. Cópias mais antigas são excluídas para garantir que o número total de snapshots ARP esteja dentro desse limite especificado. O `-option-value` parâmetro aceita inteiros entre 3 e 8, inclusive. O valor padrão é 6.
`arw.snap.create.interval.hours`	Especifica o intervalo *em horas* entre instantâneos ARP. Um novo snapshot ARP é criado quando um ataque baseado em entropia de dados é suspeito e o snapshot ARP criado mais recentemente é mais antigo do que o intervalo especificado. O `-option-value` parâmetro aceita inteiros entre 1 e 48, inclusive. O valor padrão é 4.
`arw.snap.normal.retain.interval.hours`	Especifica a duração *em horas* para a qual um instantâneo ARP é retido. Quando um instantâneo ARP atinge o limite de retenção, qualquer outra cópia de instantâneos ARP criada antes de ser excluída. Não pode existir mais do que um instantâneo ARP mais antigo do que o limite de retenção. O `-option -value` parâmetro aceita inteiros entre 4 e 96, inclusive. O valor padrão é 48.
`arw.snap.max.retain.interval.days`	Especifica a duração máxima *in Days* para a qual um instantâneo ARP pode ser retido. Qualquer snapshot ARP com mais de uma duração é excluído quando não há nenhum ataque relatado no volume. O intervalo máximo de retenção para instantâneos ARP é ignorado se uma ameaça moderada for detetada. O snapshot ARP criado em resposta à ameaça é retido até que você tenha respondido à ameaça. Quando você marca uma ameaça como um falso positivo, o ONTAP excluirá os snapshots ARP para o volume. O `-option-value` parâmetro aceita inteiros entre 1 e 365, inclusive. O valor padrão é 5.

Definição ARW	Descrição
`arw.snap.create.interval.hours.post.max.count`	Especifica o intervalo *em horas* entre instantâneos ARP quando o volume já contém o número máximo de instantâneos ARP. Quando o número máximo é atingido, um instantâneo ARP é excluído para abrir espaço para uma nova cópia. A nova velocidade de criação de instantâneos ARP pode ser reduzida para reter a cópia mais antiga usando esta opção. Se o volume já contiver o número máximo de instantâneos ARP, o intervalo especificado nesta opção será usado para a próxima criação de instantâneos ARP, em vez `arw.snap.create.interval.hours` de . O `-option-value` parâmetro aceita inteiros entre 4 e 48, inclusive. O valor padrão é 8.
`arw.surge.snap.interval.days`	Especifica o intervalo *in Days* entre instantâneos ARP criados em resposta a picos de e/S. O ONTAP cria uma cópia de impulso de snapshot ARP quando há um aumento no tráfego de e/S e o último snapshot ARP criado é mais antigo do que esse intervalo especificado. Esta opção também especifica o período de retenção *in day* para um instantâneo de pico ARP. O `-option -value` parâmetro aceita inteiros entre 1 e 365, inclusive. O valor padrão é 5.
`arw.snap.new.extns.interval.hours`	Esta opção especifica o intervalo *em horas* entre os instantâneos ARP criados quando uma nova extensão de arquivo é detetada. Um novo snapshot ARP é criado quando uma nova extensão de arquivo é observada; o snapshot anterior criado ao observar uma nova extensão de arquivo é mais antigo do que esse intervalo especificado. Em uma carga de trabalho que frequentemente cria novas extensões de arquivo, esse intervalo ajuda a controlar a frequência dos snapshots ARP. Essa opção existe independente do `arw.snap.create.interval.hours`, que especifica o intervalo para snapshots ARP baseados em entropia de dados. O `-option-value` parâmetro aceita inteiros entre 24 e 8760. O valor padrão é 48.

Proteção contra vírus com Vscan

Visão geral da configuração do antivírus

O Vscan é uma solução de verificação antivírus desenvolvida pela NetApp que permite aos clientes proteger seus dados de serem comprometidos por vírus ou outros códigos maliciosos.

O Vscan executa verificações de vírus quando os clientes acessam arquivos por SMB. Você pode configurar o Vscan para digitalizar sob demanda ou em um horário. Você pode interagir com o Vscan usando a interface de linha de comando (CLI) do ONTAP ou as interfaces de programação de aplicativos (APIs) do ONTAP.

Informações relacionadas

"Soluções de parceiros Vscan"

Sobre a proteção antivírus do NetApp

Sobre a verificação de vírus NetApp

O Vscan é uma solução de verificação antivírus desenvolvida pela NetApp que permite aos clientes proteger seus dados de serem comprometidos por vírus ou outros códigos maliciosos. Ele combina software antivírus fornecido pelo parceiro com recursos do ONTAP para dar aos clientes a flexibilidade de que precisam para gerenciar a verificação de arquivos.

Como a verificação de vírus funciona

Os sistemas de storage descarregam as operações de verificação para servidores externos que hospedam softwares antivírus de terceiros.

Com base no modo de digitalização ativo, o ONTAP envia solicitações de digitalização quando os clientes acessam arquivos por SMB (on-access) ou acessar arquivos em locais específicos, em um horário ou imediatamente (sob demanda).

- Você pode usar *verificação no acesso* para verificar se há vírus quando os clientes abrem, leem, renomeam ou fecham arquivos pelo SMB. As operações de arquivo são suspensas até que o servidor externo comunique o status de digitalização do arquivo. Se o ficheiro já tiver sido lido, o ONTAP permite a operação do ficheiro. Caso contrário, ele solicita uma verificação do servidor.

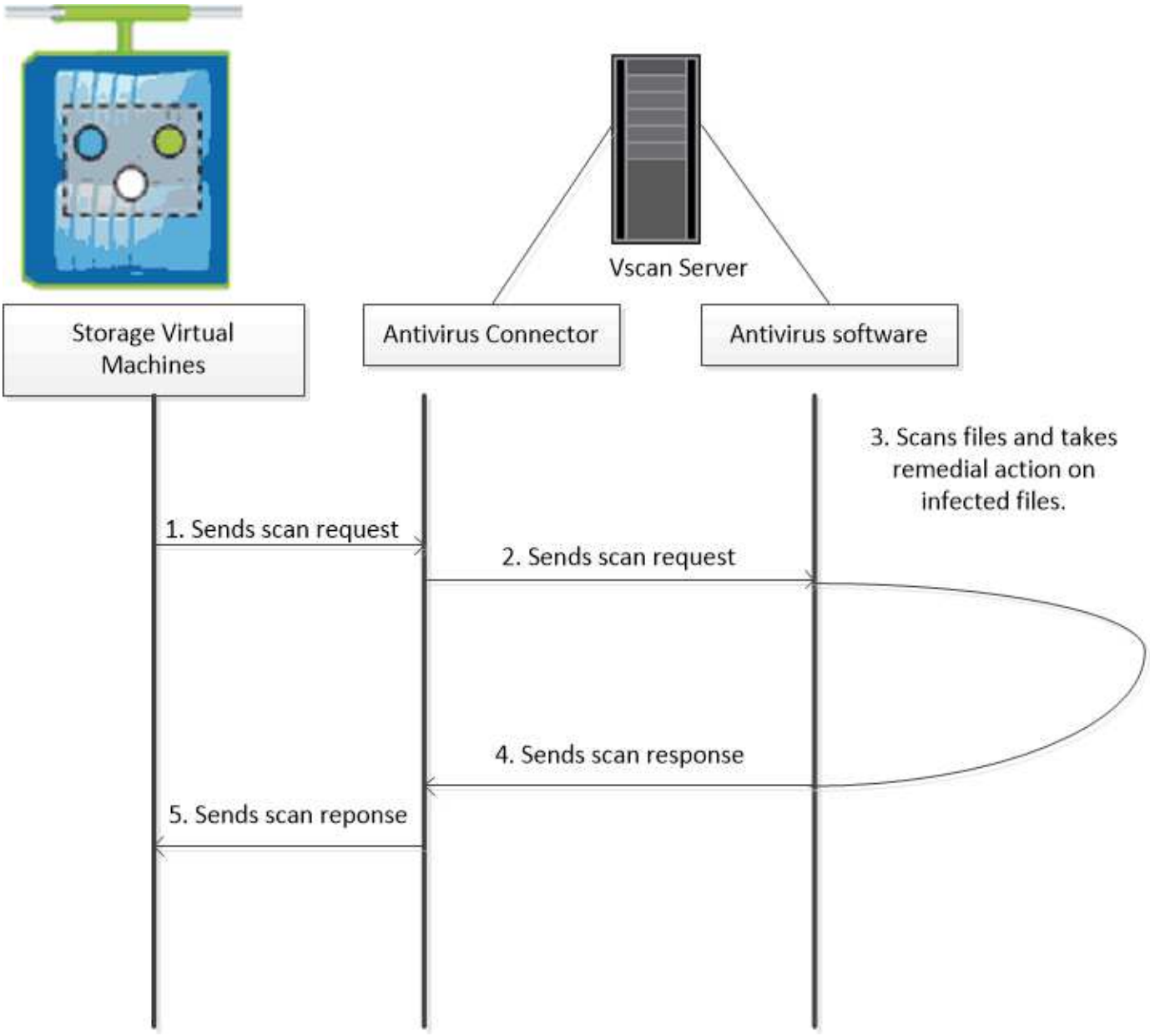
  A verificação no acesso não é suportada para NFS.

- Você pode usar *On-demand scanning* para verificar arquivos para vírus imediatamente ou em uma programação. Recomendamos que as verificações a pedido sejam executadas apenas em horas fora do pico para evitar sobrecarregar a infra-estrutura AV existente, que normalmente é dimensionada para a digitalização no acesso. O servidor externo atualiza o status de verificação dos arquivos verificados, de modo que a latência de acesso ao arquivo seja reduzida em relação ao SMB. Se houver modificações de arquivo ou atualizações de versão de software, ele solicita uma nova verificação de arquivo do servidor externo.

  Você pode usar a verificação sob demanda para qualquer caminho no namespace SVM, até mesmo para volumes exportados somente por NFS.

Normalmente, você ativa os modos de digitalização sob demanda e de acesso sob demanda em uma SVM. Em ambos os modos, o software antivírus toma medidas corretivas em arquivos infetados com base em suas configurações de software.

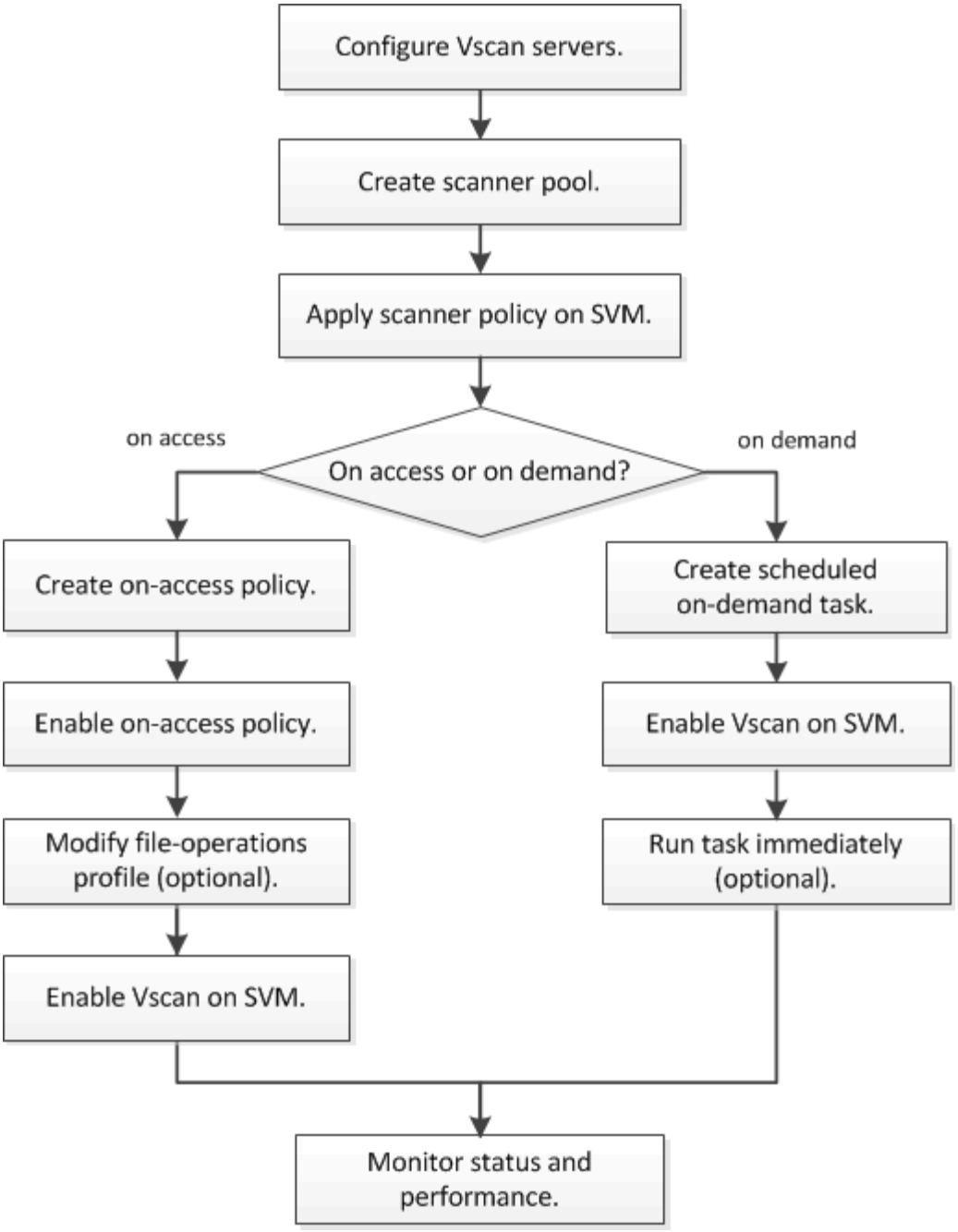
O conetor do antivírus ONTAP, fornecido pelo NetApp e instalado no servidor externo, lida com a comunicação entre o sistema de armazenamento e o software antivírus.



Fluxo de trabalho de verificação de vírus

Você deve criar um pool de scanner e aplicar uma política de scanner antes de ativar a digitalização. Normalmente, você ativa os modos de digitalização sob demanda e de acesso sob demanda em uma SVM.

Você deve ter concluído a configuração CIFS.



Para criar uma tarefa sob demanda, deve haver pelo menos uma política de acesso ativada. Pode ser a política padrão ou uma política de acesso criada pelo usuário.

Próximas etapas

- Crie um pool de scanners em um único cluster
- Aplique uma política de scanner em um único cluster
- Crie uma política de acesso

Arquitetura antivírus

A arquitetura antivírus do NetApp consiste em software de servidor Vscan e configurações associadas.

Software do servidor Vscan

Tem de instalar este software no servidor Vscan.

- **Conetor do antivírus ONTAP**

  Este é um software fornecido pela NetApp que lida com a comunicação de solicitação de verificação e resposta entre os SVMs e o software antivírus. Ele pode ser executado em uma máquina virtual, mas para o melhor desempenho use uma máquina física. Você pode baixar este software a partir do site de suporte da NetApp (requer login).

- **Software antivírus**

  Este é um software fornecido por parceiros que verifica os ficheiros em busca de vírus ou outro código malicioso. Você especifica as ações corretivas a serem tomadas em arquivos infetados ao configurar o software.

Definições do software Vscan

Tem de configurar estas definições de software no servidor Vscan.

- **Piscina do scanner**

  Esta configuração define os servidores Vscan e os usuários privilegiados que podem se conetar a SVMs. Ele também define um período de tempo limite de solicitação de digitalização, após o qual a solicitação de digitalização é enviada para um servidor Vscan alternativo, se houver um disponível.

  > Você deve definir o período de tempo limite no software antivírus no servidor Vscan para cinco segundos a menos do que o período de tempo limite de solicitação de digitalização do pool do scanner. Isso evitará situações em que o acesso ao arquivo seja atrasado ou negado completamente porque o período de tempo limite no software é maior do que o período de tempo limite para a solicitação de digitalização.

- **Usuário privilegiado**

  Essa configuração é uma conta de usuário de domínio que um servidor Vscan usa para se conetar ao SVM. A conta deve existir na lista de utilizadores privilegiados no conjunto do scanner.

- **Política do scanner**

  Esta definição determina se um conjunto de scanners está ativo. As políticas do scanner são definidas pelo sistema, pelo que não é possível criar políticas personalizadas do scanner. Apenas estas três políticas estão disponíveis:

  - `Primary` especifica que o pool do scanner está ativo.
  - `Secondary` Especifica que o pool de scanner está ativo, somente quando nenhum dos servidores Vscan no pool de scanner primário estiver conetado.
  - `Idle` especifica que o conjunto de scanners está inativo.

- **Política de acesso**

  Esta definição define o âmbito de uma digitalização no acesso. Pode especificar o tamanho máximo do ficheiro a analisar, as extensões e os caminhos de ficheiro a incluir na digitalização e as extensões e caminhos de ficheiro a excluir da digitalização.

Por padrão, somente os volumes de leitura e gravação são digitalizados. Você pode especificar filtros que permitem a digitalização de volumes somente leitura ou que restringem a digitalização a arquivos abertos com acesso de execução:

- `scan-ro-volume` permite a digitalização de volumes só de leitura.
- `scan-execute-access` restringe a digitalização para arquivos abertos com acesso de execução.

> "Execute Access" é diferente de "execute permission". Um determinado cliente terá "execute access" em um arquivo executável somente se o arquivo tiver sido aberto com "execute intent".

Você pode definir a `scan-mandatory` opção como Desativado para especificar que o acesso ao arquivo é permitido quando nenhum servidor Vscan estiver disponível para verificação de vírus. No modo de acesso, pode escolher entre estas duas opções mutuamente exclusivas:

- Obrigatório: Com esta opção, o Vscan tenta entregar a solicitação de digitalização ao servidor até que o período de tempo limite expire. Se a solicitação de digitalização não for aceita pelo servidor, a solicitação de acesso do cliente será negada.
- Não obrigatório: Com esta opção, o Vscan sempre permite o acesso do cliente, independentemente de um servidor Vscan estar ou não disponível para verificação de vírus.

- **Tarefa sob demanda**

Esta definição define o âmbito de uma digitalização a pedido. Pode especificar o tamanho máximo do ficheiro a analisar, as extensões e os caminhos de ficheiro a incluir na digitalização e as extensões e caminhos de ficheiro a excluir da digitalização. Os arquivos nos subdiretórios são verificados por padrão.

Você usa um cronograma cron para especificar quando a tarefa é executada. Você pode usar o `vserver vscan on-demand-task run` comando para executar a tarefa imediatamente.

- **Perfil de operações de arquivo Vscan (somente digitalização no acesso)**

O `vscan-fileop-profile` parâmetro para `vserver cifs share create` o comando define quais operações de arquivo SMB acionam a verificação de vírus. Por padrão, o parâmetro é definido como `standard`, que é a melhor prática do NetApp. Você pode ajustar esse parâmetro conforme necessário ao criar ou modificar um compartilhamento SMB:

- `no-scan` especifica que as verificações de vírus nunca são acionadas para o compartilhamento.
- `standard` especifica que as verificações de vírus são acionadas por operações abertas, fechadas e renomeadas.
- `strict` especifica que as verificações de vírus são acionadas por operações abertas, lidas, fechadas e renomeadas.

  O `strict` perfil fornece segurança aprimorada para situações em que vários clientes acessam um arquivo simultaneamente. Se um cliente fechar um arquivo depois de gravar um vírus para ele, e o mesmo arquivo permanecer aberto em um segundo cliente, `strict` garante que uma operação de leitura no segundo cliente aciona uma verificação antes que o arquivo seja fechado.

  Você deve ter cuidado para restringir o `strict` perfil a compartilhamentos contendo arquivos que você espera que serão acessados simultaneamente. Uma vez que este perfil gera mais pedidos de digitalização, pode afetar o desempenho.

- `writes-only` especifica que as verificações de vírus são acionadas apenas quando os arquivos modificados são fechados.

  Como `writes-only` gera menos solicitações de digitalização, geralmente melhora o desempenho.

Se você usar esse perfil, o scanner deve estar configurado para excluir ou colocar em quarentena arquivos infetados não reparáveis, para que eles não possam ser acessados. Se, por exemplo, um cliente fechar um arquivo depois de gravar um vírus para ele, e o arquivo não for reparado, excluído ou em quarentena, qualquer cliente que acesse a gravação do arquivo `without` para ele será infetado.

Se um aplicativo cliente executar uma operação de renomeação, o arquivo será fechado com o novo nome e não será digitalizado. Se tais operações representarem uma preocupação de segurança no seu ambiente, deve utilizar o `standard` perfil ou `strict`.

Soluções de parceiros Vscan

A NetApp colabora com Trellix, Symantec, Trend Micro e Sentinel One para oferecer soluções anti-malware e antivírus líderes do setor, baseadas na tecnologia ONTAP Vscan. Essas soluções ajudam você a verificar arquivos em busca de malware e corrigir quaisquer arquivos afetados.

Como mostrado na tabela abaixo, os detalhes de interoperabilidade para Trellix, Symantec e Trend Micro são mantidos na Matriz de interoperabilidade do NetApp. Os detalhes de interoperabilidade para Trellix e Symantec também podem ser encontrados nos sites de parceiros. Os detalhes de interoperabilidade para o Sentinel One e outros novos parceiros serão mantidos pelo parceiro em seus sites.

Parceiro	Documentação da solução	Detalhes de interoperabilidade
Trellix (anteriormente McAfee)	"Documentação do produto Trellix"	• "Ferramenta de Matriz de interoperabilidade do NetApp" • "Plataformas compatíveis para proteção de armazenamento de segurança de endpoints (trellix.com)"
Symantec	"Symantec Protection Engine 9.0.0"	• "Ferramenta de Matriz de interoperabilidade do NetApp" • "Matriz de suporte para dispositivos parceiros certificados com Symantec Protection Engine (SPE) para armazenamento conetado à rede (nas) 9.x.x" • "Matriz de suporte para dispositivos de parceiros certificados com Symantec Protection Engine (SPE) para armazenamento conetado à rede (nas) 8.x (broadcom.com)"

Parceiro	Documentação da solução	Detalhes de interoperabilidade
Trend Micro	"Guia de introdução do Trend Micro ServerProtect for Storage 6,0"	"Ferramenta de Matriz de interoperabilidade do NetApp"
Sentinel One	• "SentinelOne Singularity Segurança de dados na nuvem" • "Suporte ao SentinelOne" Este link requer um login de usuário. Você pode solicitar acesso a partir do Sentinel One.	Deep Instinct
Deep Instinct Prevention for Storage • "Documentação e Interop" Este link requer um login de usuário. Você pode solicitar acesso do Deep Instinct. • "Folha de dados"	OPSWAT	OPSWAT MetaDefender Storage Security • "Integração de segurança de armazenamento MetaDefender com o NetApp" • "Página de parceiros OPSWAP" • "Resumo da solução de integração"

Instalação e configuração do servidor Vscan

Instalação e configuração do servidor Vscan

Configure um ou mais servidores Vscan para garantir que os arquivos no seu sistema sejam verificados por vírus. Siga as instruções fornecidas pelo fornecedor para instalar e configurar o software antivírus no servidor.

Siga as instruções no arquivo README fornecido pelo NetApp para instalar e configurar o conetor antivírus do ONTAP. Em alternativa, siga as instruções na "Instale a página do conetor antivírus do ONTAP".

Para a recuperação de desastres e configurações do MetroCluster, é necessário configurar servidores Vscan separados para os clusters ONTAP primário, local e secundário/parceiro.

Requisitos de software antivírus

- Para obter informações sobre os requisitos de software antivírus, consulte a documentação do fornecedor.
- Para obter informações sobre os fornecedores, software e versões compatíveis com o Vscan, consulte a "Soluções de parceiros Vscan" página.

Requisitos do conetor antivírus do ONTAP

- Você pode baixar o conetor antivírus da ONTAP na página **Download de software** no site de suporte da NetApp. "Downloads de NetApp: Software"

- Para obter informações sobre as versões do Windows suportadas pelo conetor antivírus do ONTAP e os requisitos de interoperabilidade, "Soluções de parceiros Vscan"consulte .

> Você pode instalar versões diferentes de servidores Windows para diferentes servidores Vscan em um cluster.

- .NET 3,0 ou posterior deve ser instalado no servidor Windows.
- O SMB 2,0 deve estar ativado no servidor Windows.

Instale o conetor antivírus do ONTAP

Instale o conetor do antivírus ONTAP no servidor Vscan para permitir a comunicação entre o sistema que executa o ONTAP e o servidor Vscan. Quando o conetor antivírus do ONTAP é instalado, o software antivírus consegue se comunicar com uma ou mais máquinas virtuais de armazenamento (SVMs).

Sobre esta tarefa

- Consulte a "Soluções de parceiros Vscan" página para obter informações sobre os protocolos suportados, versões de software de fornecedores de antivírus, versões do ONTAP, requisitos de interoperabilidade e servidores Windows.
- .NET 4.5.1 ou posterior deve ser instalado.
- O conetor do antivírus ONTAP pode ser executado em uma máquina virtual. No entanto, para obter o melhor desempenho, a NetApp recomenda o uso de uma máquina física dedicada para verificação de antivírus.
- O SMB 2,0 deve estar habilitado no servidor Windows no qual você está instalando e executando o conetor antivírus do ONTAP.

Antes de começar

- Faça o download do arquivo de configuração do conetor antivírus do ONTAP no site de suporte e salve-o em um diretório no disco rígido.
- Verifique se você atende aos requisitos para instalar o conetor antivírus do ONTAP.
- Verifique se você tem o Privileges administrador para instalar o conetor antivírus.

Passos

1. Inicie o assistente de instalação do Antivirus Connector executando o arquivo de configuração apropriado.
2. Selecione *Next*. Abre-se a caixa de diálogo pasta de destino.
3. Selecione *Next* para instalar o conetor antivírus na pasta listada ou selecione *Change* para instalar em uma pasta diferente.
4. A caixa de diálogo credenciais de serviço do Windows do conetor AV do ONTAP é aberta.
5. Insira suas credenciais de serviço do Windows ou selecione **Adicionar** para selecionar um usuário. Para um sistema ONTAP, esse usuário deve ser um usuário de domínio válido e deve existir na configuração do pool do scanner para o SVM.
6. Selecione **seguinte**. A caixa de diálogo Pronto para instalar o programa é aberta.
7. Selecione **Instalar** para iniciar a instalação ou selecione **voltar** se quiser fazer alterações nas configurações. Uma caixa de status é aberta e mostra o andamento da instalação, seguida pela caixa de diálogo Assistente InstallShield concluído.

8. Marque a caixa de seleção Configurar LIFs do ONTAP se desejar continuar com a configuração do gerenciamento do ONTAP ou LIFs de dados. Você deve configurar pelo menos um ONTAP Management ou data LIF antes que este servidor Vscan possa ser usado.
9. Marque a caixa de seleção Mostrar o log **Windows Installer** se desejar exibir os logs de instalação.
10. Selecione **Finish** para terminar a instalação e fechar o assistente InstallShield. O ícone **Configurar LIFs ONTAP** é salvo na área de trabalho para configurar os LIFs ONTAP.
11. Adicione um SVM ao Antivirus Connector. Você pode adicionar um SVM ao conetor do antivírus adicionando um LIF de gerenciamento do ONTAP, que é polled para recuperar a lista de LIFs de dados ou configurando diretamente o LIF ou LIFs de dados. Você também deve fornecer as informações da enquete e as credenciais da conta de administrador do ONTAP se o LIF de gerenciamento do ONTAP estiver configurado.
    - Verifique se o LIF de gerenciamento ou o endereço IP do SVM está habilitado para `management-https`. Isso não é necessário quando você está configurando apenas LIFs de dados.
    - Verifique se você criou uma conta de usuário para o aplicativo HTTP e atribuiu uma função que tem (pelo menos somente leitura) acesso à `/api/network/ip/interfaces` API REST.
    - Saiba mais sobre os comandos `security login role create`(em inglês) e link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-create.html[`security login create`na referência de comando ONTAP.

> Você também pode usar o usuário do domínio como uma conta adicionando um túnel de autenticação SVM para um SVM administrativo. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-domain-tunnel-create.html[`security login domain-tunnel create` em referência de comando ONTAP.

Passos

1. Clique com o botão direito do Mouse no ícone **Configurar LIFs ONTAP**, que foi salvo em sua área de trabalho quando você concluiu a instalação do conetor antivírus e selecione **Executar como Administrador**.
2. Na caixa de diálogo Configurar LIFs ONTAP , selecione o tipo de configuração preferencial e execute as seguintes ações:

Para criar este tipo de LIF…	Execute estas etapas…
LIF de dados	a. Definir "função" para "dados" b. Definir "protocolo de dados" para "cifs" c. Defina "política de firewall" como "dados" d. Defina "Service policy" como "default-data-files" (ficheiros de dados predefinidos)
LIF de gerenciamento	a. Definir "função* como "dados" b. Defina "data Protocol" (protocolo de dados) para "None" (nenhum) c. Defina "política de firewall" como "mgmt" d. Defina "Service policy" (política de serviço) para "Default-Management" (gestão predefinida)

Leia mais sobre "Criando um LIF".

Depois de criar um LIF, insira os dados ou LIF de gerenciamento ou endereço IP do SVM que você deseja adicionar. Você também pode inserir o LIF de gerenciamento de cluster. Se você especificar o LIF de gerenciamento de cluster, todos os SVMs dentro desse cluster que estão atendendo SMB podem usar o servidor Vscan.

> Quando a autenticação Kerberos é necessária para servidores Vscan, cada LIF de dados SVM deve ter um nome DNS exclusivo e você deve Registrar esse nome como um nome principal do servidor (SPN) no ative Directory do Windows. Quando um nome DNS exclusivo não está disponível para cada LIF de dados ou registrado como um SPN, o servidor Vscan usa o mecanismo NT LAN Manager para autenticação. Se você adicionar ou modificar os nomes DNS e SPNs depois que o servidor Vscan estiver conetado, reinicie o serviço Antivirus Connector no servidor Vscan para aplicar as alterações.

3. Para configurar um LIF de gerenciamento, insira a duração da pesquisa em segundos. A duração da enquete é a frequência na qual o conetor antivírus verifica as alterações nas SVMs ou na configuração LIF do cluster. O intervalo padrão da enquete é de 60 segundos.
4. Introduza o nome e a palavra-passe da conta de administrador do ONTAP para configurar um LIF de gestão.
5. Clique em **Test** para verificar a conetividade e verificar a autenticação. A autenticação é verificada apenas para uma configuração de LIF de gerenciamento.
6. Clique em **Atualizar** para adicionar o LIF à lista de LIFs à pesquisa ou ao qual se conetar.
7. Clique em **Salvar** para salvar a conexão ao Registro.
8. Clique em **Exportar** se quiser exportar a lista de conexões para um arquivo de importação ou exportação de Registro. Isso é útil se vários servidores Vscan usarem o mesmo conjunto de gerenciamento ou LIFs de dados.

Consulte "Configure a página do conetor do antivírus ONTAP"para obter as opções de configuração.

Configure o conetor do antivírus ONTAP

Configure o conetor antivírus do ONTAP para especificar uma ou mais máquinas virtuais de armazenamento (SVMs) às quais você deseja se conetar, inserindo o LIF de gerenciamento do ONTAP, as informações de enquete e as credenciais da conta de administrador do ONTAP ou apenas o LIF de dados. Você também pode modificar os detalhes de uma conexão SVM ou remover uma conexão SVM. Por padrão, o conetor antivírus do ONTAP usa APIS REST para recuperar a lista de LIFs de dados se o LIF de gerenciamento do ONTAP estiver configurado.

Modifique os detalhes de uma conexão SVM

Você pode atualizar os detalhes de uma conexão de máquina virtual de armazenamento (SVM), que foi adicionada ao conetor antivírus, modificando o LIF de gerenciamento do ONTAP e as informações de enquete. Não é possível atualizar LIFs de dados depois de adicionados. Para atualizar LIFs de dados, primeiro você deve removê-los e adicioná-los novamente com o novo endereço IP ou LIF.

Antes de começar

Verifique se você criou uma conta de usuário para o aplicativo HTTP e atribuiu uma função que tem (pelo menos somente leitura) acesso à `/api/network/ip/interfaces` API REST.

Saiba mais sobre os comandos link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-role-create.html[`security login role create` e link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-create.html[`security login create` em referência de comando ONTAP.

Você também pode usar o usuário do domínio como uma conta adicionando um túnel de autenticação SVM para um SVM administrativo. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-domain-tunnel-create.html[`security login domain-tunnel create` em referência de comando ONTAP.

Passos

1. Clique com o botão direito do Mouse no ícone **Configurar LIFs ONTAP**, que foi salvo em sua área de trabalho quando você concluiu a instalação do conetor antivírus e selecione **Executar como Administrador**. A caixa de diálogo Configurar LIFs ONTAP será aberta.
2. Selecione o endereço IP SVM e clique em **Update**.
3. Atualize as informações, conforme necessário.
4. Clique em **Salvar** para atualizar os detalhes da conexão no Registro.
5. Clique em **Exportar** se quiser exportar a lista de conexões para uma importação de Registro ou um arquivo de exportação de Registro. Isso é útil se vários servidores Vscan usarem o mesmo conjunto de gerenciamento ou LIFs de dados.

Remova uma conexão SVM do Antivirus Connector

Se você não precisar mais de uma conexão SVM, poderá removê-la.

Passos

1. Clique com o botão direito do Mouse no ícone **Configurar LIFs ONTAP**, que foi salvo em sua área de trabalho quando você concluiu a instalação do conetor antivírus e selecione **Executar como Administrador**. A caixa de diálogo Configurar LIFs ONTAP será aberta.
2. Selecione um ou mais endereços IP SVM e clique em **Remover**.
3. Clique em **Salvar** para atualizar os detalhes da conexão no Registro.
4. Clique em **Exportar** se quiser exportar a lista de conexões para um arquivo de importação ou exportação de Registro. Isso é útil se vários servidores Vscan usarem o mesmo conjunto de gerenciamento ou LIFs de dados.

Solucionar problemas

Antes de começar

Quando estiver criando valores de Registro neste procedimento, use o painel direito.

Você pode ativar ou desativar os logs do Antivirus Connector para fins de diagnóstico. Por padrão, esses logs são desativados. Para um melhor desempenho, você deve manter os logs do Antivirus Connector desabilitados e apenas habilitá-los para eventos críticos.

Passos

1. Selecione **Iniciar**, digite "regedit" na caixa de pesquisa e selecione `regedit.exe` na lista programas.
2. Em **Editor de Registro**, localize a seguinte subchave para o conetor antivírus do ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Crie valores de Registro fornecendo o tipo, nome e valores mostrados na tabela a seguir:

Tipo	Nome	Valores
Cadeia de carateres	Tracepath	c: avshim.log

Este valor de registo pode ser qualquer outro caminho válido.

4. Crie outro valor de Registro fornecendo o tipo, nome, valores e informações de Registro mostradas na tabela a seguir:

Tipo	Nome	Registo crítico	Registo intermédio	Registro detalhado
DWORD	Tracelevel	1	2 ou 3	4

Isso permite que os logs do conetor antivírus sejam salvos no valor de caminho fornecido no TracePath na Etapa 3.

5. Desative os logs do Antivirus Connector excluindo os valores de Registro criados nas etapas 3 e 4.
6. Crie outro valor de Registro do tipo "MULTI_SZ" com o nome "LogRotation" (sem aspas). Em "LogRotation", forneça "logFileSize:1" como uma entrada para o tamanho de rotação (onde 1 representa 1MB) e na linha seguinte, forneça "logFileCount:5" como uma entrada para o limite de rotação (5 é o limite).

> Estes valores são opcionais. Se eles não forem fornecidos, os valores padrão de arquivos 20MB e 10 serão usados para o tamanho de rotação e limite de rotação, respetivamente. Os valores inteiros fornecidos não fornecem valores decimais ou frações. Se você fornecer valores superiores aos valores padrão, os valores padrão serão usados.

7. Para desativar a rotação de log configurada pelo usuário, exclua os valores do Registro criados na Etapa 6.

Banner personalizável

Um banner personalizado permite que você coloque uma declaração juridicamente vinculativa e uma isenção de responsabilidade de acesso ao sistema na janela *Configurar ONTAP API*.

Passo

1. Modifique o banner padrão atualizando o conteúdo do `banner.txt` arquivo no diretório de instalação e salvando as alterações. É necessário reabrir a janela Configurar API ONTAP LIF para ver as alterações refletidas no banner.

Ativar o modo de Ordenação alargada (eo)

Você pode ativar e desativar o modo Extended Ordinance (eo) para operação segura.

Passos

1. Selecione **Iniciar**, digite "regedit" na caixa de pesquisa e selecione `regedit.exe` na lista programas.
2. Em **Editor de Registro**, localize a seguinte subchave para o conetor antivírus do ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. No painel do lado direito, crie um novo valor de Registro do tipo "DWORD" com o nome "eo_Mode" (sem

aspas) e o valor "1" (sem aspas) para ativar o modo eo ou o valor "0" (sem aspas) para desativar o modo eo.

Por padrão, se a `EO_Mode` entrada do Registro estiver ausente, o modo eo será desativado. Ao ativar o modo eo, você deve configurar tanto o servidor syslog externo quanto a autenticação mútua de certificados.

Configure o servidor syslog externo

Antes de começar

Observe que quando você estiver criando valores de Registro neste procedimento, use o painel do lado direito.

Passos

1. Selecione **Iniciar**, digite "regedit" na caixa de pesquisa e selecione `regedit.exe` na lista programas.
2. Em **Editor de Registro**, crie a seguinte subchave para o conetor antivírus do ONTAP para configuração syslog:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Crie um valor de Registro fornecendo o tipo, nome e valor, conforme mostrado na tabela a seguir:

Tipo	Nome	Valor
DWORD	syslog_enabled	1 ou 0

   Observe que um valor "1" ativa o syslog e um valor "0" o desativa.

4. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome
REG_SZ	Syslog_host

   Forneça o endereço IP do host syslog ou o nome de domínio para o campo valor.

5. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome
REG_SZ	Syslog_port

   Forneça o número da porta na qual o servidor syslog está sendo executado no campo valor.

6. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome
REG_SZ	Syslog_Protocol

Insira o protocolo que está em uso no servidor syslog, "tcp" ou "udp", no campo valor.

7. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome	Valor
DWORD	syslog_tls	1 ou 0

Observe que um valor "1" ativa o syslog com Transport Layer Security (TLS) e um valor "0" desabilita o syslog com TLS.

Certifique-se de que um servidor syslog externo configurado seja executado sem problemas

- Se a chave estiver ausente ou tiver um valor nulo:
  - O protocolo é predefinido para "tcp".
  - A porta padrão é "514" para "tcp/udp" e padrão é "6514" para TLS.
  - O nível syslog é padrão para 5 (LOG_NOTICE).
- Você pode confirmar que o syslog está habilitado verificando se o `syslog_enabled` valor é "1". Quando o `syslog_enabled` valor é "1", você deve ser capaz de fazer login no servidor remoto configurado, quer o modo eo esteja ou não ativado.
- Se o modo eo estiver definido para "1" e alterar o `syslog_enabled` valor de "1" para "0", aplica-se o seguinte:
  - Não é possível iniciar o serviço se o syslog não estiver ativado no modo eo.
  - Se o sistema estiver sendo executado em um estado estável, um aviso aparece dizendo que syslog não pode ser desativado no modo eo e syslog está definido com força para "1", o que você pode ver no Registro. Se isso ocorrer, você deve desativar o modo eo primeiro e, em seguida, desativar syslog.
- Se o servidor syslog não conseguir executar com êxito quando o modo eo e syslog estão ativados, o serviço pára de ser executado. Isso pode ocorrer por um dos seguintes motivos:
  - Um syslog_host inválido ou nenhum syslog_host está configurado.
  - Um protocolo inválido, além de UDP ou TCP, está configurado.
  - Um número de porta é inválido.
- Para uma configuração TCP ou TLS sobre TCP, se o servidor não estiver escutando na porta IP, a conexão falhará e o serviço será encerrado.

Configurar a autenticação de certificado mútuo X,509

A autenticação mútua baseada em certificado X,509 é possível para a comunicação SSL (Secure Sockets Layer) entre o conetor antivírus e o ONTAP no caminho de gerenciamento. Se o modo eo estiver ativado e o certificado não for encontrado, o conetor AV será encerrado. Execute o seguinte procedimento no Antivirus Connector:

Passos

1. O conetor do antivírus procura o certificado do cliente do conetor do antivírus e o certificado da autoridade de certificação (CA) para o servidor NetApp no caminho do diretório a partir do qual o conetor do antivírus executa o diretório de instalação. Copie os certificados para este caminho de diretório fixo.
2. Incorpore o certificado do cliente e sua chave privada no formato PKCS12 e nomeie-o "AV_client.P12".
3. Certifique-se de que o certificado de CA (juntamente com qualquer autoridade de assinatura intermediária até a CA raiz) usado para assinar o certificado para o servidor NetApp esteja no formato de email avançado de privacidade (PEM) e chamado "ONTAP_CA.pem". Coloque-o no diretório de instalação do conetor do antivírus. No sistema NetApp ONTAP, instale o certificado CA (juntamente com qualquer autoridade de assinatura intermediária até a CA raiz) usado para assinar o certificado de cliente para o conetor antivírus em "ONTAP" como um certificado de tipo "cliente-CA".

Configurar pools do scanner

Configure a visão geral dos pools de scanner

Um pool de scanners define os servidores Vscan e os usuários privilegiados que podem se conetar a SVMs. Uma política de scanner determina se um pool de scanner está ativo.

Se utilizar uma política de exportação num servidor SMB, tem de adicionar cada servidor Vscan à política de exportação.

Crie um pool de scanners em um único cluster

Um pool de scanners define os servidores Vscan e os usuários privilegiados que podem se conetar a SVMs. Você pode criar um pool de varredor para uma SVM individual ou para todos os SVMs em um cluster.

O que você vai precisar

- Os servidores SVMs e Vscan devem estar no mesmo domínio ou em domínios confiáveis.
- Para pools de scanners definidos para SVM individual, você precisa ter o ONTAP Antivirus Connector configurado com o SVM Management LIF ou LIF de dados SVM.
- Para pools de scanners definidos para todos os SVMs em um cluster, você deve ter configurado o conetor antivírus ONTAP com o LIF de gerenciamento de cluster.
- A lista de usuários privilegiados deve incluir a conta de usuário do domínio que o servidor Vscan usa para se conetar ao SVM.
- Depois que o pool do scanner estiver configurado, verifique o status da conexão com os servidores.

Passos

1. Criar um conjunto de scanners:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

   - Especifique um SVM de dados para um pool definido para um SVM individual e especifique um SVM admin de cluster para um pool definido para todas as SVMs em um cluster.

- Especifique um endereço IP ou FQDN para cada nome de host do servidor Vscan.
- Especifique o domínio e o nome de usuário para cada usuário privilegiado. Para obter uma lista completa de opções, consulte a página de manual do comando.

  O comando a seguir cria um pool de scanner chamado `SP` na `vs1` SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Verifique se o conjunto do scanner foi criado:

   `vserver vscan scanner-pool show -vserver` *data_SVM*|*cluster_admin_SVM* `-scanner -pool` *scanner_pool*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes do `SP` pool do scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
          Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

   Você também pode usar o `vserver vscan scanner-pool show` comando para exibir todos os pools de scanner em um SVM. Para obter a sintaxe de comando completa, consulte a página man para o comando.

Crie pools de scanner nas configurações do MetroCluster

É necessário criar pools de scanners primários e secundários em cada cluster em uma configuração do MetroCluster, correspondendo aos SVMs primárias e secundárias no cluster.

O que você vai precisar

- Os servidores SVMs e Vscan devem estar no mesmo domínio ou em domínios confiáveis.
- Para pools de scanners definidos para SVM individual, você precisa ter o ONTAP Antivirus Connector

configurado com o SVM Management LIF ou LIF de dados SVM.

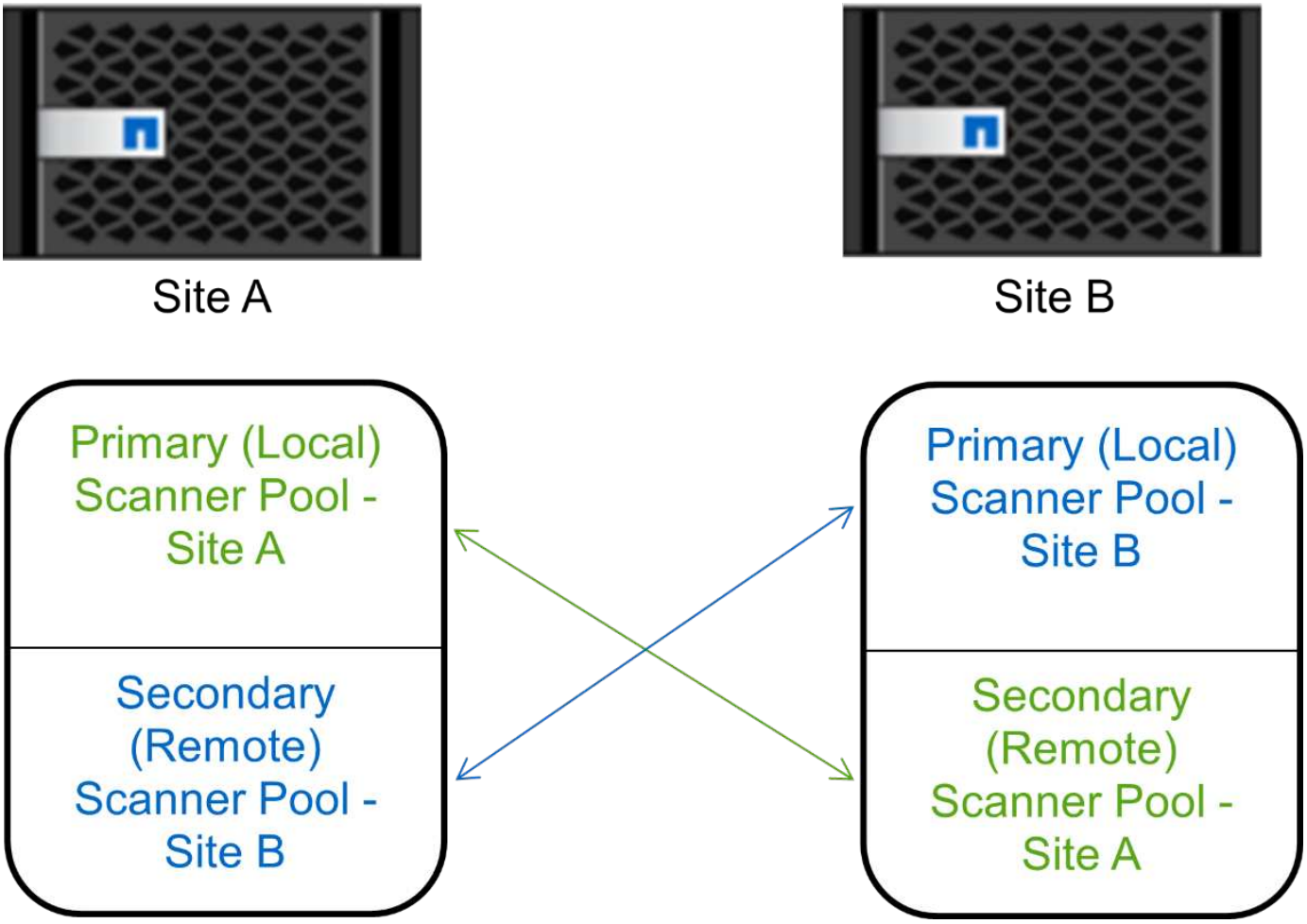
- Para pools de scanners definidos para todos os SVMs em um cluster, você deve ter configurado o conetor antivírus ONTAP com o LIF de gerenciamento de cluster.
- A lista de usuários privilegiados deve incluir a conta de usuário do domínio que o servidor Vscan usa para se conetar ao SVM.
- Depois que o pool do scanner estiver configurado, verifique o status da conexão com os servidores.

Sobre esta tarefa

As configurações do MetroCluster protegem os dados com a implementação de dois clusters espelhados separados fisicamente. Cada cluster replica de forma síncrona os dados e a configuração da SVM do outro. Um SVM principal no cluster local serve dados quando o cluster está on-line. Um SVM secundário no cluster local serve dados quando o cluster remoto está off-line.

Isso significa que você precisa criar pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster. O pool secundário fica ativo quando o cluster começa a fornecer dados do SVM secundário. Para recuperação de desastres (DR), a configuração é semelhante ao MetroCluster.

Esta figura mostra uma configuração típica de MetroCluster/DR.



Passos

1. Criar um conjunto de scanners:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
```

`-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users`

- Especifique um SVM de dados para um pool definido para um SVM individual e especifique um SVM admin de cluster para um pool definido para todas as SVMs em um cluster.
- Especifique um endereço IP ou FQDN para cada nome de host do servidor Vscan.
- Especifique o domínio e o nome de usuário para cada usuário privilegiado.

> É necessário criar todos os pools de scanner a partir do cluster que contém o SVM principal.

Para obter uma lista completa de opções, consulte a página de manual do comando.

Os comandos a seguir criam pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verifique se os pools do scanner foram criados:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes do pool do scanner `pool1` :

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

Você também pode usar o `vserver vscan scanner-pool show` comando para exibir todos os pools de scanner em um SVM. Para obter a sintaxe de comando completa, consulte a página man para o comando.

Aplique uma política de scanner em um único cluster

Uma política de scanner determina se um pool de scanner está ativo. Você deve ativar um pool de scanner antes que os servidores Vscan que ele define possam se conetar a um SVM.

Sobre esta tarefa

- Só é possível aplicar uma política de scanner a um conjunto de scanners.
- Se você criou um pool de scanners para todos os SVMs em um cluster, deverá aplicar uma política de scanner a cada SVM individualmente.

Passos

1. Aplicar uma política de scanner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Uma política de scanner pode ter um dos seguintes valores:

   - `Primary` especifica que o pool do scanner está ativo.
   - `Secondary` Especifica que o conjunto de scanners está ativo apenas se nenhum dos servidores Vscan no conjunto de scanners primário estiver conetado.
   - `Idle` especifica que o conjunto de scanners está inativo.

   O exemplo a seguir mostra que o pool do scanner chamado `SP` na `vs1` SVM está ativo:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. Verifique se o conjunto do scanner está ativo:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes do `SP` pool do scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: primary
                             Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

   Você pode usar o `vserver vscan scanner-pool show-active` comando para exibir os pools de scanner ativos em um SVM. Para obter a sintaxe completa do comando, consulte a página man para o comando.

Aplique políticas de scanner nas configurações do MetroCluster

Uma política de scanner determina se um pool de scanner está ativo. Você deve aplicar uma política de scanner aos pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster.

Sobre esta tarefa

- Só é possível aplicar uma política de scanner a um conjunto de scanners.
- Se você criou um pool de scanners para todos os SVMs em um cluster, deverá aplicar uma política de scanner a cada SVM individualmente.
- Para configurações de recuperação de desastres e MetroCluster, você deve aplicar uma política de scanner a cada pool de scanners no cluster local e no cluster remoto.
- Na política criada para o cluster local, tem de especificar o cluster local no `cluster` parâmetro. Na política criada para o cluster remoto, tem de especificar o cluster remoto no `cluster` parâmetro. O cluster remoto pode então assumir operações de verificação de vírus em caso de desastre.

Passos

1. Aplicar uma política de scanner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Uma política de scanner pode ter um dos seguintes valores:

   - `Primary` especifica que o pool do scanner está ativo.
   - `Secondary` Especifica que o conjunto de scanners está ativo apenas se nenhum dos servidores Vscan no conjunto de scanners primário estiver conetado.
   - `Idle` especifica que o conjunto de scanners está inativo.

   > É necessário aplicar todas as políticas de scanner a partir do cluster que contém o SVM principal.

   Os comandos a seguir aplicam políticas de scanner aos pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster:

   ```
   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
   cluster1

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
   cluster2
   ```

2. Verifique se o conjunto do scanner está ativo:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes do pool do scanner `pool1` :

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

Você pode usar o `vserver vscan scanner-pool show-active` comando para exibir os pools de scanner ativos em um SVM. Para obter a sintaxe de comando completa, consulte a página man para o comando.

Comandos para gerenciar pools de scanner

Você pode modificar e excluir pools de scanner e gerenciar usuários privilegiados e servidores Vscan para um pool de scanner. Você também pode exibir informações resumidas sobre o pool do scanner.

Se você quiser…	Digite o seguinte comando…
Modifique um conjunto de scanners	`vserver vscan scanner-pool modify`
Exclua um pool de scanner	`vserver vscan scanner-pool delete`
Adicione usuários privilegiados a um pool de scanners	`vserver vscan scanner-pool privileged-users add`
Excluir usuários privilegiados de um pool de scanner	`vserver vscan scanner-pool privileged-users remove`
Adicione servidores Vscan a um pool de scanners	`vserver vscan scanner-pool servers add`
Excluir servidores Vscan de um pool de scanners	`vserver vscan scanner-pool servers remove`
Exibir resumo e detalhes de um pool de scanners	`vserver vscan scanner-pool show`
Exibir usuários privilegiados de um pool de scanners	`vserver vscan scanner-pool privileged-users show`

Veja os servidores Vscan para todos os pools de scanners	`vserver vscan scanner-pool servers show`

Para obter mais informações sobre esses comandos, consulte as páginas man.

Configurar a digitalização no acesso

Crie uma política de acesso

Uma política de acesso define o escopo de uma digitalização no acesso. Você pode criar uma política de acesso para um SVM individual ou para todos os SVMs em um cluster. Se você criou uma política de acesso para todos os SVMs em um cluster, habilite a política em cada SVM individualmente.

Sobre esta tarefa

- Pode especificar o tamanho máximo do ficheiro a analisar, as extensões e os caminhos de ficheiro a incluir na digitalização e as extensões e caminhos de ficheiro a excluir da digitalização.
- Você pode definir a `scan-mandatory` opção como Desativado para especificar que o acesso ao arquivo é permitido quando nenhum servidor Vscan estiver disponível para verificação de vírus.
- Por padrão, o ONTAP cria uma política de acesso chamada "default_CIFS" e a habilita para todos os SVMs em um cluster.
- Qualquer arquivo que se qualifica para exclusão de digitalização com base nos `paths-to-exclude` parâmetros , , `file-ext-to-exclude` ou `max-file-size` não é considerado para digitalização, mesmo que a `scan-mandatory` opção esteja definida como ativado. (Verifique "solução de problemas"esta seção para problemas de conetividade relacionados à `scan-mandatory` opção.)
- Por padrão, somente os volumes de leitura e gravação são digitalizados. Você pode especificar filtros que ativam a digitalização de volumes somente leitura ou que restringem a digitalização a arquivos abertos com acesso de execução.
- A verificação de vírus não é realizada em um compartilhamento SMB para o qual o parâmetro continuamente disponível está definido como Sim.
- Consulte "Arquitetura antivírus"a seção para obter detalhes sobre o perfil *Vscan file-operations*.
- Você pode criar um máximo de dez (10) políticas de acesso por SVM. No entanto, você pode ativar apenas uma política de acesso por vez.
  - Você pode excluir um máximo de cem (100) caminhos e extensões de arquivo da verificação de vírus em uma política de acesso.
- Algumas recomendações de exclusão de arquivos:
  - Considere excluir arquivos grandes (o tamanho do arquivo pode ser especificado) da verificação de vírus, porque eles podem resultar em uma resposta lenta ou tempos limite de solicitações de verificação para usuários CIFS. O tamanho padrão do arquivo para exclusão é 2GB.
  - Considere excluir extensões de arquivo como `.vhd` e `.tmp` porque arquivos com essas extensões podem não ser apropriados para a digitalização.
  - Considere excluir caminhos de arquivo, como o diretório de quarentena ou caminhos nos quais apenas discos rígidos virtuais ou bancos de dados são armazenados.
  - Verifique se todas as exclusões estão especificadas na mesma política, pois somente uma diretiva pode ser ativada de cada vez. A NetApp recomenda vivamente que tenha o mesmo conjunto de

exclusões especificado no mecanismo antivírus.

- É necessária uma política de acesso para um digitalização a pedido. Para evitar a digitalização no acesso, você deve definir `-scan-files-with-no-ext` como false e `-file-ext-to-exclude` como * para excluir todas as extensões.

Passos

1. Crie uma política de acesso:

   `vserver vscan on-access-policy create -vserver` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`policy_name`* `-protocol CIFS -max-file-size` *`max_size_of_files_to_scan`* `-filters [scan-ro-volume,][scan-execute-access] -file-ext-to-include` *`extensions_of_files_to_include`* `-file-ext-to-exclude` *`extensions_of_files_to_exclude`* `-scan-files-with-no-ext true|false -paths-to -exclude` *`paths_of_files_to_exclude`* `-scan-mandatory on|off`

   - Especifique um SVM de dados para uma política definida para um SVM individual, um administrador de cluster SVM para uma política definida para todos os SVMs em um cluster.
   - A `-file-ext-to-exclude` definição substitui a `-file-ext-to-include` definição.
   - Defina `-scan-files-with-no-ext` como verdadeiro para digitalizar arquivos sem extensões. O comando a seguir cria uma política de acesso denominada `Policy1` na `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. Verifique se a política de acesso foi criada: `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes da `Policy1` política:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Ative uma política de acesso

Uma política de acesso define o escopo de uma digitalização no acesso. Você deve habilitar uma política de acesso em um SVM antes que seus arquivos possam ser digitalizados.

Se você criou uma política de acesso para todos os SVMs em um cluster, habilite a política em cada SVM individualmente. Você pode ativar apenas uma política de acesso em um SVM de cada vez.

Passos

1. Ativar uma política de acesso:

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   O comando a seguir habilita uma política de acesso denominada `Policy1` na `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. Verifique se a política de acesso está ativada:

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes da `Policy1` política de acesso:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Modifique o perfil de operações de arquivo Vscan para um compartilhamento SMB

O perfil *Vscan file-operations* de um compartilhamento SMB define as operações no compartilhamento que podem acionar a digitalização. Por padrão, o parâmetro é definido como `standard`. Você pode ajustar o parâmetro conforme necessário ao criar ou modificar um compartilhamento SMB.

Consulte "Arquitetura antivírus"a seção para obter detalhes sobre o perfil *Vscan file-operations*.

> A verificação de vírus não é realizada em um compartilhamento SMB que tenha o `continuously-available` parâmetro definido como `Yes`.

Passo

1. Modifique o valor do perfil de operações de ficheiros Vscan para uma partilha SMB:

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir altera o perfil de operações do arquivo Vscan para um compartilhamento SMB para `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

Comandos para gerenciar políticas de acesso

Você pode modificar, desativar ou excluir uma política de acesso. Você pode exibir um

resumo e detalhes da política.

Se você quiser…	Digite o seguinte comando…
Crie uma política de acesso	`vserver vscan on-access-policy create`
Modificar uma política de acesso	`vserver vscan on-access-policy modify`
Ative uma política de acesso	`vserver vscan on-access-policy enable`
Desative uma política de acesso	`vserver vscan on-access-policy disable`
Eliminar uma política de acesso	`vserver vscan on-access-policy delete`
Veja o resumo e os detalhes de uma política de acesso	`vserver vscan on-access-policy show`
Adicionar à lista de caminhos a excluir	`vserver vscan on-access-policy paths-to-exclude add`
Excluir da lista de caminhos a serem excluídos	`vserver vscan on-access-policy paths-to-exclude remove`
Exibir a lista de caminhos a serem excluídos	`vserver vscan on-access-policy paths-to-exclude show`
Adicionar à lista de extensões de arquivo a excluir	`vserver vscan on-access-policy file-ext-to-exclude add`
Excluir da lista de extensões de arquivo a serem excluídas	`vserver vscan on-access-policy file-ext-to-exclude remove`
Veja a lista de extensões de arquivo a excluir	`vserver vscan on-access-policy file-ext-to-exclude show`
Adicionar à lista de extensões de arquivo a incluir	`vserver vscan on-access-policy file-ext-to-include add`
Excluir da lista de extensões de arquivo a incluir	`vserver vscan on-access-policy file-ext-to-include remove`
Veja a lista de extensões de arquivo a incluir	`vserver vscan on-access-policy file-ext-to-include show`

Para obter mais informações sobre esses comandos, consulte as páginas man.

Configurar a digitalização a pedido

Configure a visão geral da digitalização a pedido

Você pode usar a verificação sob demanda para verificar arquivos para vírus imediatamente ou em um horário.

Você pode querer executar digitalizações apenas em horas fora do pico, por exemplo, ou você pode querer digitalizar arquivos muito grandes que foram excluídos de uma digitalização no acesso. Você pode usar um cronograma cron para especificar quando a tarefa é executada.

> Para criar uma tarefa sob demanda, deve haver pelo menos uma política de acesso ativada. Pode ser a política padrão ou uma política de acesso criada pelo usuário.

Sobre este tópico

- Você pode atribuir um agendamento ao criar uma tarefa.
- Somente uma tarefa pode ser agendada de cada vez em um SVM.
- A digitalização sob demanda não suporta a digitalização de links simbólicos ou arquivos de fluxo.

> A digitalização sob demanda não suporta a digitalização de links simbólicos ou arquivos de fluxo.

> Para criar uma tarefa sob demanda, deve haver pelo menos uma política de acesso ativada. Pode ser a política padrão ou uma política de acesso criada pelo usuário.

Crie uma tarefa sob demanda

Uma tarefa sob demanda define o escopo da verificação de vírus sob demanda. Pode especificar o tamanho máximo dos ficheiros a digitalizar, as extensões e os caminhos dos ficheiros a incluir na digitalização e as extensões e caminhos dos ficheiros a excluir da digitalização. Os arquivos nos subdiretórios são verificados por padrão.

Sobre esta tarefa

- Pode existir no máximo 10 (dez) tarefas sob demanda para cada SVM, mas apenas uma pode estar ativa.
- Uma tarefa a pedido cria um relatório, que tem informações sobre as estatísticas relacionadas com as digitalizações. Este relatório é acessível com um comando ou baixando o arquivo de relatório criado pela tarefa no local definido.

Antes de começar

- Você deve ter criou uma política de acesso. A política pode ser uma política padrão ou criada pelo usuário. Sem a política de acesso, não é possível ativar a digitalização.

Passos

1. Crie uma tarefa sob demanda:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
```

`-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with -no-ext true|false -directory-recursion true|false`

- A `-file-ext-to-exclude` definição substitui a `-file-ext-to-include` definição.
- Defina `-scan-files-with-no-ext` como verdadeiro para digitalizar arquivos sem extensões.

  Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-vscan-on-demand-task-create.html[`vserver vscan on-demand-task create` em referência de comando ONTAP.

  O comando a seguir cria uma tarefa sob demanda chamada `Task1` no SVM VS1:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> Pode utilizar o `job show` comando para visualizar o estado do trabalho. Pode utilizar os `job pause` comandos e `job resume` para pausar e reiniciar o trabalho ou o `job stop` comando para terminar o trabalho.

2. Verifique se a tarefa a pedido foi criada:

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes `Task1` da tarefa:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                 List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
        Expiration Time for Report: -
```

Depois de terminar

Você deve habilitar a digitalização no SVM antes que a tarefa seja agendada para ser executada.

Agende uma tarefa sob demanda

Você pode criar uma tarefa sem atribuir uma programação e usar o `vserver vscan on-demand-task schedule` comando para atribuir uma programação; ou adicionar uma programação ao criar a tarefa.

Sobre esta tarefa

A programação atribuída com o `vserver vscan on-demand-task schedule` comando substitui uma programação já atribuída com o `vserver vscan on-demand-task create` comando.

Passos

1. Agendar uma tarefa a pedido:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   O comando a seguir agenda uma tarefa de acesso chamada `Task2` no `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

Para ver o estado do trabalho, utilize o `job show` comando . Os `job pause` comandos e `job resume`, respetivamente, pausam e reiniciam a tarefa; o `job stop` comando termina a tarefa.

2. Verifique se a tarefa a pedido foi agendada:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe os detalhes `Task 2` da tarefa:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
```

Depois de terminar

Você deve habilitar a digitalização no SVM antes que a tarefa seja agendada para ser executada.

Execute uma tarefa sob demanda imediatamente

Você pode executar uma tarefa sob demanda imediatamente, independentemente de ter atribuído ou não uma programação.

Antes de começar

Você deve ter habilitado a verificação na SVM.

Passo

1. Execute uma tarefa sob demanda imediatamente:

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   O comando a seguir executa uma tarefa de acesso chamada `Task1` no `vs1` SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

Pode utilizar o `job show` comando para visualizar o estado do trabalho. Pode utilizar os `job pause` comandos e `job resume` para pausar e reiniciar o trabalho ou o `job stop` comando para terminar o trabalho.

Comandos para gerenciar tarefas sob demanda

Você pode modificar, excluir ou desagendar uma tarefa sob demanda. Você pode exibir um resumo e detalhes da tarefa e gerenciar relatórios para a tarefa.

Se você quiser…	Digite o seguinte comando…
Crie uma tarefa sob demanda	`vserver vscan on-demand-task create`
Modifique uma tarefa sob demanda	`vserver vscan on-demand-task modify`
Eliminar uma tarefa a pedido	`vserver vscan on-demand-task delete`
Execute uma tarefa sob demanda	`vserver vscan on-demand-task run`
Agende uma tarefa sob demanda	`vserver vscan on-demand-task schedule`
Anule a programação de uma tarefa sob demanda	`vserver vscan on-demand-task unschedule`
Exibir resumo e detalhes de uma tarefa sob demanda	`vserver vscan on-demand-task show`
Veja relatórios sob demanda	`vserver vscan on-demand-task report show`
Eliminar relatórios a pedido	`vserver vscan on-demand-task report delete`

Para obter mais informações sobre esses comandos, consulte as páginas man.

Práticas recomendadas para configurar a funcionalidade antivírus off-box no ONTAP

Considere as seguintes recomendações para configurar a funcionalidade off-box no ONTAP.

- Restringir usuários privilegiados a operações de verificação de vírus. Os usuários normais devem ser desencorajados a usar credenciais de usuário privilegiadas. Essa restrição pode ser alcançada desativando os direitos de login para usuários privilegiados no ative Directory.
- Os usuários privilegiados não precisam fazer parte de nenhum grupo de usuários que tenha um grande número de direitos no domínio, como o grupo administradores ou o grupo de operadores de backup. Os usuários privilegiados devem ser validados apenas pelo sistema de armazenamento para que eles possam criar conexões de servidor Vscan e acessar arquivos para verificação de vírus.
- Use os computadores que executam servidores Vscan apenas para fins de verificação de vírus. Para desencorajar o uso geral, desative os serviços de terminal do Windows e outras disposições de acesso remoto nessas máquinas e conceda o direito de instalar novos softwares nessas máquinas somente aos administradores.
- Dedique os servidores Vscan à verificação de vírus e não os use para outras operações, como backups. Você pode decidir executar o servidor Vscan como uma máquina virtual (VM). Se você executar o servidor Vscan como uma VM, certifique-se de que os recursos alocados à VM não sejam compartilhados e sejam suficientes para executar a verificação de vírus.
- Fornecer CPU, memória e capacidade de disco adequados ao servidor Vscan para evitar a alocação excessiva de recursos. A maioria dos servidores Vscan são projetados para usar vários servidores centrais da CPU e para distribuir a carga entre as CPUs.
- A NetApp recomenda o uso de uma rede dedicada com uma VLAN privada para a conexão do SVM ao servidor Vscan para que o tráfego de varredura não seja afetado por outro tráfego de rede cliente. Crie uma placa de interface de rede (NIC) separada dedicada à VLAN antivírus no servidor Vscan e ao LIF de dados na SVM. Esta etapa simplifica a administração e a solução de problemas se surgirem problemas de rede. O tráfego antivírus deve ser segregado usando uma rede privada. O servidor antivírus deve ser configurado para se comunicar com o controlador de domínio (DC) e o ONTAP de uma das seguintes maneiras:
  - O DC deve se comunicar com os servidores antivírus através da rede privada que é usada para segregar o tráfego.
  - O DC e o servidor antivírus devem se comunicar através de uma rede diferente (não a rede privada mencionada anteriormente), que não é a mesma que a rede cliente CIFS.
  - Para ativar a autenticação Kerberos para comunicação antivírus, crie uma entrada DNS para os LIFs privados e um nome principal de serviço no DC correspondente à entrada DNS criada para o LIF privado. Use esse nome ao adicionar um LIF ao conetor do antivírus. O DNS deve ser capaz de retornar um nome exclusivo para cada LIF privado conetado ao conetor Antivirus.

Se o LIF para tráfego Vscan for configurado em uma porta diferente do LIF para tráfego de cliente, o Vscan LIF pode falhar para outro nó se ocorrer uma falha de porta. A alteração faz com que o servidor Vscan não seja acessível a partir do novo nó e as notificações de digitalização para operações de arquivo no nó falharem. Verifique se o servidor Vscan está acessível através de pelo menos um LIF em um nó para que ele possa processar solicitações de digitalização para operações de arquivo executadas nesse nó.

- Conete o sistema de armazenamento NetApp e o servidor Vscan usando pelo menos uma rede 1GbEG.
- Para um ambiente com vários servidores Vscan, conete todos os servidores com conexões de rede semelhantes de alto desempenho. Conetar os servidores Vscan melhora o desempenho permitindo o compartilhamento de carga.
- Para locais remotos e filiais, a NetApp recomenda o uso de um servidor Vscan local em vez de um servidor Vscan remoto porque o primeiro é um candidato perfeito para alta latência. Se o custo for um fator, use um laptop ou PC para proteção moderada contra vírus. Você pode agendar verificações periódicas completas do sistema de arquivos compartilhando os volumes ou qtrees e digitalizando-os a

partir de qualquer sistema no local remoto.

- Use vários servidores Vscan para verificar os dados no SVM para fins de balanceamento de carga e redundância. A quantidade de carga de trabalho CIFS e o tráfego antivírus resultante variam de acordo com a SVM. Monitore a latência de CIFS e verificação de vírus no controlador de storage. Monitore a tendência dos resultados ao longo do tempo. Se a latência CIFS e a latência de verificação de vírus aumentarem devido às filas de CPU ou de aplicativos nos servidores Vscan além dos limites de tendência, os clientes CIFS podem ter longos tempos de espera. Adicione servidores Vscan adicionais para distribuir a carga.
- Instale a versão mais recente do ONTAP Antivirus Connector.
- Mantenha os mecanismos e definições antivírus atualizados. Consulte os parceiros para obter recomendações sobre a frequência com que você deve atualizar.
- Em um ambiente de alocação a vários clientes, um pool de scanners (pool de servidores Vscan) pode ser compartilhado com vários SVMs, desde que os servidores Vscan e os SVMs façam parte do mesmo domínio ou domínio confiável.
- A política de software antivírus para arquivos infetados deve ser definida como "excluir" ou "quarentena", que é o valor padrão definido pela maioria dos fornecedores de antivírus. Se o "vscan-fileop-profile" estiver definido como "write_only", e se um arquivo infetado for encontrado, o arquivo permanece no compartilhamento e pode ser aberto porque a abertura de um arquivo não aciona uma verificação. A verificação antivírus é acionada apenas depois de o ficheiro ser fechado.
- O `scan-engine timeout` valor deve ser inferior ao `scanner-pool request-timeout` valor. Se estiver definido para um valor mais alto, o acesso aos arquivos pode ser atrasado e eventualmente acabar. Para evitar isso, configure o `scan-engine timeout` para 5 segundos menos do que o `scanner-pool request-timeout` valor. Consulte a documentação do fornecedor do mecanismo de digitalização para obter instruções sobre como alterar as `scan-engine timeout` configurações. O `scanner-pool timeout` pode ser alterado usando o seguinte comando no modo avançado e fornecendo o valor apropriado para o `request-timeout` parâmetro:
`vserver vscan scanner-pool modify`.
- Para um ambiente dimensionado para cargas de trabalho de verificação de acesso e que exija o uso da verificação sob demanda, a NetApp recomenda agendar o trabalho de verificação sob demanda em horas fora do horário de pico para evitar cargas adicionais na infraestrutura antivírus existente.

Saiba mais sobre as práticas recomendadas específicas dos parceiros em "Soluções de parceiros Vscan".

Ative a verificação de vírus em um SVM

Você deve habilitar a verificação de vírus em uma SVM antes de uma verificação sob demanda ou de acesso poder ser executada.

Passos

1. Ativar a verificação de vírus em um SVM:

   ```
   vserver vscan enable -vserver data_SVM
   ```

   > Você pode usar o `vserver vscan disable` comando para desativar a verificação de vírus, se necessário.

   O seguinte comando permite a verificação de vírus na `vs1` SVM:

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Verifique se a verificação de vírus está ativada na SVM:

   `vserver vscan show -vserver data_SVM`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe o status Vscan do `vs1` SVM:

```
cluster1::> vserver vscan show -vserver vs1

                           Vserver: vs1
                      Vscan Status: on
```

Repor o estado dos ficheiros lidos

Ocasionalmente, você pode querer redefinir o status de digitalização de arquivos digitalizados com êxito em um SVM usando o `vserver vscan reset` comando para descartar as informações em cache dos arquivos. Você pode querer usar este comando para reiniciar o processamento de verificação de vírus em caso de uma verificação mal configurada, por exemplo.

Sobre esta tarefa

Depois de executar o `vserver vscan reset` comando, todos os arquivos elegíveis serão verificados da próxima vez que forem acessados.

> Este comando pode afetar negativamente o desempenho, dependendo do número e tamanho dos arquivos a serem regravados.

Antes de começar

São necessários Privileges avançados para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   `set -privilege advanced`

2. Repor o estado dos ficheiros lidos:

   `vserver vscan reset -vserver data_SVM`

   O comando a seguir redefine o status dos arquivos digitalizados `vs1` no SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

Ver informações do registo de eventos Vscan

Você pode usar o `vserver vscan show-events` comando para exibir informações de log de eventos sobre arquivos infetados, atualizações para servidores Vscan e similares. Você pode exibir informações de eventos para o cluster ou para determinados nós, SVMs ou servidores Vscan.

Antes de começar

São necessários Privileges avançados para visualizar o registo de eventos Vscan.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ver informações do registo de eventos Vscan:

   ```
   vserver vscan show-events
   ```

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir exibe informações de log de eventos para o cluster `cluster1`:

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type        Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

Monitore e solucione problemas de conetividade

Potenciais problemas de conetividade envolvendo a opção de digitalização obrigatória

Você pode usar os `vserver vscan connection-status show` comandos para exibir informações sobre as conexões do servidor Vscan que você pode achar útil na solução de problemas de conetividade.

Por padrão, a `scan-mandatory` opção de digitalização no acesso nega o acesso aos arquivos quando uma conexão do servidor Vscan não está disponível para digitalização. Embora esta opção ofereça caraterísticas de segurança importantes, pode levar a problemas em algumas situações.

- Antes de ativar o acesso do cliente, você deve garantir que pelo menos um servidor Vscan esteja conetado a um SVM em cada nó que tenha um LIF. Se você precisar conetar servidores a SVMs depois de habilitar o acesso ao cliente, desative a `scan-mandatory` opção no SVM para garantir que o acesso ao arquivo não seja negado porque uma conexão com o servidor Vscan não está disponível. Você pode ativar a opção novamente depois que o servidor tiver sido conetado.
- Se um LIF de destino hospedar todas as conexões do servidor Vscan para um SVM, a conexão entre o servidor e o SVM será perdida se o LIF for migrado. Para garantir que o acesso ao arquivo não seja negado porque uma conexão de servidor Vscan não está disponível, você deve desativar a `scan-mandatory` opção antes de migrar o LIF. Você pode ativar a opção novamente após a migração do LIF.

Cada SVM deve ter pelo menos dois servidores Vscan atribuídos a ele. É uma prática recomendada conetar servidores Vscan ao sistema de armazenamento através de uma rede diferente da usada para acesso ao cliente.

Comandos para visualizar o estado da ligação do servidor Vscan

Pode utilizar os `vserver vscan connection-status show` comandos para visualizar informações resumidas e detalhadas sobre o estado da ligação do servidor Vscan.

Se você quiser…	Digite o seguinte comando…
Ver um resumo das ligações do servidor Vscan	`vserver vscan connection-status show`
Ver detalhes das ligações do servidor Vscan	`vserver vscan connection-status show-all`
Ver detalhes dos servidores Vscan ligados	`vserver vscan connection-status show-connected`
Ver detalhes dos servidores Vscan disponíveis que não estão ligados	`vserver vscan connection-status show-not-connected`

Para obter mais informações sobre esses comandos, consulte "Páginas de manual do ONTAP".

Solucionar problemas de verificação de vírus

Para problemas comuns de verificação de vírus, existem possíveis causas e maneiras de resolvê-los. A verificação de vírus também é conhecida como Vscan.

Problema	Como resolvê-lo

Os servidores Vscan não conseguem se conetar ao sistema de armazenamento ONTAP em cluster.	Verifique se a configuração do conjunto do scanner especifica o endereço IP do servidor Vscan. Verifique também se os utilizadores privilegiados permitidos na lista de conjuntos de scanners estão ativos. Para verificar o conjunto do scanner, execute o `vserver vscan scanner-pool show` comando no prompt de comando do sistema de armazenamento. Se os servidores Vscan ainda não puderem se conetar, pode haver um problema com a rede.
Os clientes observam alta latência.	Provavelmente é hora de adicionar mais servidores Vscan ao pool do scanner.
Demasiados exames são acionados.	Modifique o valor `vscan-fileop-profile` do parâmetro para restringir o número de operações de arquivo monitoradas para verificação de vírus.
Alguns ficheiros não estão a ser lidos.	Verifique a política de acesso. É possível que o caminho para esses arquivos tenha sido adicionado à lista de exclusão de caminho ou que seu tamanho exceda o valor configurado para exclusões. Para verificar a política de acesso, execute o `vserver vscan on-access-policy show` comando no prompt de comando do sistema de armazenamento.
O acesso ao ficheiro foi negado.	Verifique se a definição *scan-mandatory* está especificada na configuração da política. Esta configuração nega o acesso aos dados se nenhum servidor Vscan estiver conetado. Modifique a configuração conforme necessário.

Monitorar as atividades de status e desempenho

Você pode monitorar os aspetos críticos do módulo Vscan, como o status da conexão do servidor Vscan, a integridade dos servidores Vscan e o número de arquivos verificados. Estas informações ajudam-no a diagnosticar problemas relacionados com o servidor Vscan.

Veja as informações de conexão do servidor Vscan

Pode visualizar o estado da ligação dos servidores Vscan para gerir as ligações que já estão a ser utilizadas e as ligações que estão disponíveis para utilização. Vários comandos exibem informações sobre o status da conexão dos servidores Vscan.

Comando…	Informações exibidas…
`vserver vscan connection-status show`	Resumo do estado da ligação

`vserver vscan connection-status show-all`	Informações detalhadas sobre o estado da ligação
`vserver vscan connection-status show-not-connected`	Estado das ligações disponíveis mas não ligadas
`vserver vscan connection-status show-connected`	Informações sobre o servidor Vscan conetado

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Ver estatísticas do servidor Vscan

Você pode visualizar estatísticas específicas do servidor Vscan para monitorar o desempenho e diagnosticar problemas relacionados à verificação de vírus. Você deve coletar uma amostra de dados antes de usar o `statistics show` comando para exibir as estatísticas do servidor Vscan. Para concluir um exemplo de dados, execute o seguinte passo:

Passo

1. Executar o `statistics start` comando e o `optional statistics` comando STOP.

Exibir estatísticas para solicitações e latências de servidor Vscan

Você pode usar contadores ONTAP `offbox_vscan` por SVM para monitorar a taxa de solicitações do servidor Vscan que são enviadas e recebidas por segundo e as latências de servidor em todos os servidores Vscan. Para visualizar estas estatísticas, execute o seguinte passo:

Passo

1. Execute o comando statistics show `object offbox_vscan -instance SVM` com os seguintes contadores:

Contador…	Informações exibidas…
`scan_request_dispatched_rate`	Número de solicitações de verificação de vírus enviadas do ONTAP para os servidores Vscan por segundo
`scan_noti_received_rate`	Número de solicitações de verificação de vírus recebidas de volta pelo ONTAP a partir dos servidores Vscan por segundo
`dispatch_latency`	Latência no ONTAP para identificar um servidor Vscan disponível e enviar a solicitação para esse servidor Vscan
`scan_latency`	Latência de ida e volta do ONTAP para o servidor Vscan, incluindo o tempo para a digitalização ser executada

Exemplo de estatísticas geradas a partir de um contador vscan ONTAP offbox

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

Exibir estatísticas para solicitações e latências individuais de servidor Vscan

Você pode usar contadores ONTAP `offbox_vscan_server` em um servidor Vscan por SVM, por servidor Vscan e por nó para monitorar a taxa de solicitações de servidor Vscan enviadas e a latência do servidor em cada servidor Vscan individualmente. Para coletar essas informações, execute o seguinte passo:

Passo

1. Execute o `statistics show –object offbox_vscan –instance SVM:servername:nodename` comando com os seguintes contadores:

Contador…	Informações exibidas…
`scan_request_dispatched_rate`	Número de solicitações de verificação de vírus enviadas do ONTAP
`scan_latency`	Latência de ida e volta do ONTAP para o servidor Vscan, incluindo o tempo para a digitalização ser executada para os servidores Vscan por segundo

Exemplo de estatísticas geradas a partir de um contador ONTAP offbox_vscan_Server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

Exibir estatísticas para a utilização do servidor Vscan

Você também pode usar contadores ONTAP `offbox_vscan_server` para coletar estatísticas de utilização do servidor Vscan. Essas estatísticas são rastreadas por SVM, por servidor Vscan e por nó. Eles incluem utilização de CPU no servidor Vscan, profundidade de fila para operações de digitalização no servidor Vscan (atual e máximo), memória usada e rede usada. Essas estatísticas são encaminhadas pelo conetor antivírus para os contadores de estatísticas dentro do ONTAP. Eles são baseados em dados que são polidos a cada 20 segundos e devem ser coletados várias vezes para precisão; caso contrário, os valores vistos nas estatísticas refletem apenas a última sondagem. A utilização da CPU e as filas são particularmente importantes para monitorar e analisar. Um valor alto para uma fila média pode indicar que o servidor Vscan tem um gargalo. Para coletar estatísticas de utilização do servidor Vscan por SVM, por servidor Vscan e por nó, execute a seguinte etapa:

Passo

1. Colete estatísticas de utilização para o servidor Vscan

   Execute o `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` comando com os `offbox_vscan_server` seguintes contadores:

Contador…	Informações exibidas…
`scanner_stats_pct_cpu_used`	Utilização da CPU no servidor Vscan
`scanner_stats_pct_input_queue_avg`	Fila média de pedidos de leitura no servidor Vscan
`scanner_stats_pct_input_queue_hiwaterma rk`	Fila de pico de pedidos de leitura no servidor Vscan
`scanner_stats_pct_mem_used`	Memória utilizada no servidor Vscan
`scanner_stats_pct_network_used`	Rede utilizada no servidor Vscan

Exemplo de estatísticas de utilização para o servidor Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

Diretrizes de endurecimento do ONTAP

Visão geral do fortalecimento da segurança do ONTAP

O ONTAP fornece um conjunto de controles que permitem proteger o sistema operacional de storage ONTAP, o software de gerenciamento de dados líder do setor. Use as orientações e as configurações do ONTAP para ajudar sua organização a cumprir os objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

A evolução do cenário atual de ameaças apresenta uma organização com desafios únicos para proteger seus ativos mais valiosos: Dados e informações. As ameaças e vulnerabilidades avançadas e dinâmicas que enfrentamos estão cada vez mais aumentando em sofisticação. Juntamente com um aumento na eficácia das técnicas de ofuscação e reconhecimento por parte de potenciais intrusos, os gestores de sistemas devem abordar a segurança de dados e informações de forma proativa.

A partir de julho de 2024, o conteúdo de relatórios técnicos publicados anteriormente como PDFs foi integrado à documentação do produto ONTAP. A documentação de segurança do ONTAP agora inclui conteúdo de *TR-4569: Guia de proteção de segurança para ONTAP*.

Validação de imagem ONTAP

O ONTAP fornece mecanismos para garantir que a imagem ONTAP seja válida na atualização e no momento da inicialização.

Atualizar validação de imagem

A assinatura de código ajuda a verificar se as imagens ONTAP instaladas por meio de atualizações de imagem sem interrupções ou atualizações automatizadas de imagem sem interrupções, CLIs ou APIs ONTAP

são autenticamente produzidas pela NetApp e não foram adulteradas. A validação da imagem de atualização foi introduzida no ONTAP 9.3.

Esse recurso é um aprimoramento de segurança sem toque para atualização ou reversão do ONTAP. Não se espera que o usuário faça nada de diferente, exceto para opcionalmente verificar a assinatura de nível superior `image.tgz`.

Validação de imagem no momento da inicialização

A partir do ONTAP 9.4, a inicialização segura da interface de firmware extensível unificada (UEFI) é ativada para sistemas NetApp AFF A800, AFF A220, FAS2750 e FAS2720 e sistemas subsequentes de próxima geração que utilizam BIOS UEFI.

Durante a ativação, o bootloader valida o banco de dados da lista de permissões de chaves de inicialização seguras com a assinatura associada a cada módulo carregado. Depois que cada módulo é validado e carregado, o processo de inicialização continua com a inicialização do ONTAP. Se a validação da assinatura falhar para qualquer módulo, o sistema será reinicializado.

Esses itens se aplicam às imagens do ONTAP e ao BIOS da plataforma.

Contas de administrador de armazenamento local

Funções, aplicativos e autenticação

O ONTAP fornece à empresa com consciência de segurança a capacidade de fornecer acesso granular a diferentes administradores por meio de diferentes aplicativos e métodos de login. Isso ajuda os clientes a criar um modelo de confiança zero centrado nos dados.

Estas são as funções disponíveis para administradores de máquinas virtuais de administração e armazenamento. Os métodos de aplicação de início de sessão e os métodos de autenticação de início de sessão são especificados.

Funções

Com o controle de acesso baseado em funções (RBAC), os usuários têm acesso apenas aos sistemas e opções necessários para suas funções e funções de trabalho. A solução RBAC no ONTAP limita o acesso administrativo dos usuários ao nível concedido para sua função definida, o que permite que os administradores gerenciem os usuários por função atribuída. O ONTAP fornece várias funções predefinidas. Os operadores e administradores podem criar, modificar ou excluir funções de controle de acesso personalizadas e podem especificar restrições de conta para funções específicas.

Funções predefinidas para administradores de cluster

Esta função…	Tem este nível de acesso…	Para os seguintes comandos ou diretórios de comandos
`admin`	Tudo	Todos os diretórios de comando (`DEFAULT`)

admin-no-fsa (Disponível a partir de ONTAP 9.12,1)	Leitura/escrita	• Todos os diretórios de comando (DEFAULT) • security login rest-role • security login role
Somente leitura	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	Nenhum
volume file show-disk-usage	autosupport	Tudo
• set • system node autosupport	Nenhum	Todos os outros diretórios de comando (DEFAULT)
backup	Tudo	vserver services ndmp
Somente leitura	volume	Nenhum
Todos os outros diretórios de comando (DEFAULT)	readonly	Tudo

• `security login password` Apenas para gerir a palavra-passe local da conta de utilizador e as informações das chaves • `set`	Nenhum	`security`
Somente leitura	Todos os outros diretórios de comando (`DEFAULT`)	`none`

> A `autosupport` função é atribuída à conta predefinida `autosupport`, que é usada pelo AutoSupport OnDemand. O ONTAP impede que você modifique ou exclua a `autosupport` conta. O ONTAP também impede que você atribua `autosupport` a função a outras contas de usuário.

Funções predefinidas para administradores de máquina virtual de storage (SVM)

Nome da função	Recursos
`vsadmin`	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, cópias Snapshot e arquivos • Gerenciar LUNs • Executar operações SnapLock, exceto exclusão privilegiada • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Monitorizar trabalhos • Monitore conexões de rede e interface de rede • Monitorar a integridade do SVM

`vsadmin-volume`	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, incluindo movimentos de volume • Gerencie cotas, qtrees, cópias Snapshot e arquivos • Gerenciar LUNs • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede • Monitorar a integridade do SVM
`vsadmin-protocol`	• Gerencie a senha local da própria conta de usuário e as informações chave • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Gerenciar LUNs • Monitorar a interface de rede • Monitorar a integridade do SVM
`vsadmin-backup`	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerenciar operações NDMP • Faça uma leitura/gravação de volume restaurada • Gerencie relacionamentos do SnapMirror e cópias Snapshot • Exibir volumes e informações de rede
`vsadmin-snaplock`	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, cópias Snapshot e arquivos • Executar operações SnapLock, incluindo exclusão privilegiada • Configurar protocolos: NFS e SMB • Configurar serviços: DNS, LDAP e NIS • Monitorizar trabalhos • Monitore conexões de rede e interface de rede

`vsadmin-readonly`	• Gerencie a senha local da própria conta de usuário e as informações chave • Monitorar a integridade do SVM • Monitorar a interface de rede • Visualizar volumes e LUNs • Exibir serviços e protocolos

Métodos de aplicação

O método de aplicação especifica o tipo de acesso do método de início de sessão. Os valores possíveis incluem `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, e `telnet`.

Definir este parâmetro para `service-processor` conceder ao utilizador acesso ao processador de serviço. Quando este parâmetro está definido como `service-processor`, o `-authentication-method` parâmetro tem de ser definido como `password` porque o processador de serviço suporta apenas `password` a autenticação. As contas de usuário do SVM não podem acessar o processador de serviços. Portanto, os operadores e administradores não podem usar o `-vserver` parâmetro quando este parâmetro está definido como `service-processor`.

Para restringir ainda mais o acesso ao `service-processor` use o comando `system service-processor ssh add-allowed-addresses`. O comando `system service-processor api-service` pode ser usado para atualizar as configurações e certificados.

Por motivos de segurança, o Telnet e o Shell remoto (RSH) são desativados por padrão porque o NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro. Se houver um requisito ou necessidade exclusiva para Telnet ou RSH, eles devem ser ativados.

O `security protocol modify` comando modifica a configuração existente em todo o cluster do RSH e Telnet. Ative o RSH e o Telnet no cluster definindo o campo ativado para `true`.

Métodos de autenticação

O parâmetro método de autenticação especifica o método de autenticação usado para logins.

Método de autenticação	Descrição
`cert`	Autenticação de certificado SSL
`community`	Strings de comunidade SNMP
`domain`	Autenticação do ative Directory
`nsswitch`	Autenticação LDAP ou NIS
`password`	Palavra-passe
`publickey`	Autenticação de chave pública
`usm`	Modelo de segurança do utilizador SNMP

O uso de NIS não é recomendado devido a falhas de segurança do protocolo.

A partir do ONTAP 9.3, a autenticação de dois fatores encadeada está disponível para contas SSH locais

`admin` usando `publickey` e `password` como os dois métodos de autenticação. Além do `-authentication-method` campo no `security login` comando, um novo campo chamado `-second-authentication-method` foi adicionado. `publickey`Ou `password` pode ser especificado como `-authentication-method` ou `-second-authentication-method` . No entanto, durante a autenticação SSH, a ordem é sempre `publickey` com autenticação parcial, seguida pelo prompt de senha para autenticação completa.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

Começando com ONTAP 9.4, `nsswitch` pode ser usado como um segundo método de autenticação com `publickey`.

A partir do ONTAP 9.12,1, o FIDO2 também pode ser usado para autenticação SSH usando um dispositivo de autenticação de hardware YubiKey ou outros dispositivos compatíveis com o FIDO2.

Começando com ONTAP 9.13,1:

- `domain` as contas podem ser usadas como um segundo método de autenticação com `publickey`o .
- Senha única baseada no tempo (`totp`) é uma senha temporária gerada por um algoritmo que usa a hora atual do dia como um de seus fatores de autenticação para o segundo método de autenticação.
- A revogação de chaves públicas é suportada com chaves públicas SSH, bem como certificados que serão verificados para expiração/revogação durante o SSH.

Para obter mais informações sobre autenticação multifator (MFA) para Gerenciador de sistemas, Active IQ Unified Manager e SSH da ONTAP, "TR-4647: Autenticação multifator no ONTAP 9"consulte .

Contas administrativas padrão

A conta de administrador deve ser restrita porque a função de administrador tem acesso permitido usando todos os aplicativos. A conta diag permite o acesso ao shell do sistema e deve ser reservada apenas para o suporte técnico para executar tarefas de solução de problemas.

Existem duas contas administrativas padrão: `admin` E `diag`.

As contas órfãs são um grande vetor de segurança que muitas vezes leva a vulnerabilidades, incluindo a escalação do Privileges. Estas são contas desnecessárias e não utilizadas que permanecem no repositório de contas de usuário. São principalmente contas padrão que nunca foram usadas ou para as quais senhas nunca foram atualizadas ou alteradas. Para resolver esse problema, o ONTAP suporta a remoção e renomeação de contas.

O ONTAP não pode remover ou renomear contas internas. No entanto, o NetApp recomenda bloquear quaisquer contas internas desnecessárias com o comando LOCK.

Embora as contas órfãs sejam um problema de segurança significativo, o NetApp recomenda fortemente testar o efeito da remoção de contas do repositório de contas local.

Listar contas locais

Para listar as contas locais, execute o `security login show` comando.

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                              Authentication             Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name        Locked Group
---------------- ----------- --------- ---------------- ------ -----------
admin            console     password  admin            no     no
admin            http        password  admin            no     no
admin            ontapi      password  admin            no     no
admin            service-processor password admin       no     no
admin            ssh         password  admin            no     no
autosupport      console     password  autosupport      no     no
6 entries were displayed.
```

Definir a palavra-passe da conta de diagnóstico (diag)

Uma conta de diagnóstico nomeada `diag` é fornecida com o sistema de storage. Você pode usar a `diag` conta para executar tarefas de solução de problemas no `systemshell`. A `diag` conta é a única conta que pode ser usada para acessar o systemshell através do `diag` comando `systemshell`privilegiado .

> O systemshell e a conta associada `diag` destinam-se a fins de diagnóstico de baixo nível. Seu acesso requer o nível de privilégio de diagnóstico e é reservado apenas para ser usado com orientação do suporte técnico para executar tarefas de solução de problemas. Nem a `diag` conta nem o `systemshell` destinam-se a fins administrativos gerais.

Antes de começar

Antes de aceder ao `systemshell`, tem de definir a `diag` palavra-passe da conta utilizando o `security login password` comando . Você deve usar princípios de senha fortes e alterar a `diag` senha em intervalos regulares.

Passos

1. Defina a `diag` senha do usuário da conta:

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

Verificação multi-admin

A partir do ONTAP 9.11,1, é possível usar a verificação multiadministrador (MAV) para permitir que determinadas operações, como a exclusão de volumes ou cópias Snapshot, sejam executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

A configuração do MAV consiste no seguinte:

- "Criando um ou mais grupos de aprovação de administrador."
- "Habilitando a funcionalidade de verificação de vários administradores."
- "Adicionar ou modificar regras."

Após a configuração inicial, somente os administradores de um grupo de aprovação MAV (administradores MAV) podem modificar esses elementos.

Quando o MAV está ativado, a conclusão de cada operação protegida requer três passos:

1. Quando um utilizador inicia a operação, a "a solicitação é gerada."
2. Antes de poder ser executado, o número necessário de "Os administradores do MAV devem aprovar."
3. Após a aprovação, o utilizador conclui a operação.

O MAV não se destina a ser usado com volumes ou fluxos de trabalho que envolvam automação pesada, pois cada tarefa automatizada requer aprovação antes que a operação possa ser concluída. Se você quiser usar automação e MAV juntos, a NetApp recomenda que você use consultas para operações MAV específicas. Por exemplo, você pode aplicar `volume delete` regras MAV apenas a volumes em que a automação não está envolvida e pode designar esses volumes com um esquema de nomenclatura específico.

Para obter informações mais detalhadas sobre o MAV, consulte o "Documentação de verificação de vários administradores do ONTAP".

Bloqueio de cópias snapshot

O bloqueio de cópias snapshot é uma funcionalidade do SnapLock em que as cópias Snapshot são tornadas indeléveis manual ou automaticamente, com um período de retenção na política de Snapshot de volume. O objetivo do bloqueio de cópias Snapshot é impedir que administradores desonestos ou não confiáveis excluam snapshots em sistemas ONTAP primário ou secundário.

O bloqueio de cópia Snapshot foi introduzido no ONTAP 9.12,1. O bloqueio de cópias snapshot também é conhecido como bloqueio instantâneo à prova de violação. Embora isso exija a licença SnapLock e a inicialização do relógio de conformidade, o bloqueio de cópias snapshot não está relacionado ao SnapLock Compliance ou ao SnapLock Enterprise. Não há administrador de storage confiável, assim como o SnapLock Enterprise e ele não protege a infraestrutura de storage físico subjacente, como o SnapLock Compliance. Isso é uma melhoria em relação às cópias Snapshot do SnapVaulting para um sistema secundário. A recuperação rápida de snapshots bloqueados em sistemas primários pode ser obtida para restaurar volumes corrompidos por ransomware.

Para obter mais detalhes sobre o bloqueio de cópias instantâneas, consulte "Documentação do ONTAP".

Configure o acesso à API baseado em certificado

Em vez de autenticação de ID de usuário e senha para acesso à API REST ou à API SDK de gerenciamento do NetApp ao ONTAP, a autenticação baseada em certificado deve ser usada.

> Como alternativa à autenticação baseada em certificado para API REST, use "Autenticação baseada em token OAuth 2,0".)

Você pode gerar e instalar um certificado autoassinado no ONTAP conforme descrito nestas etapas.

Passos

1. Usando OpenSSL, gere um certificado executando o seguinte comando:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

   Este comando gera um certificado público nomeado `test.pem` e uma chave privada chamada `key.out`. O nome comum, CN, corresponde ao ID de usuário do ONTAP.

2. Instale o conteúdo do certificado público no formato pem (Privacy Enhanced mail) no ONTAP executando o seguinte comando e colando o conteúdo do certificado quando solicitado:

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. Ative o ONTAP para permitir o acesso do cliente através de SSL e definir a ID do usuário para acesso à API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

No exemplo a seguir, o ID de usuário `cert_user` agora está habilitado para usar o acesso à API autenticado por certificado. Um script Python simples do SDK para gerenciamento usando `cert_user` para exibir a versão do ONTAP aparece da seguinte forma:

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

A saída do script exibe a versão do ONTAP.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Para executar a autenticação baseada em certificado com a API REST do ONTAP, execute as seguintes etapas:
   a. No ONTAP, defina a ID do usuário para acesso http:

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. No seu cliente Linux, execute o seguinte comando que produz a versão ONTAP como saída:

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

Mais informações

- "Autenticação baseada em certificado com o SDK de gerenciamento do NetApp para ONTAP".

Autenticação baseada em token ONTAP OAuth 2,0 para API REST

Como alternativa à autenticação baseada em certificado, você pode usar a autenticação baseada em token OAuth 2,0 para API REST.

A partir do ONTAP 9.14,1, você tem a opção de controlar o acesso aos clusters do ONTAP usando a estrutura autorização aberta (OAuth 2,0). Você pode configurar esse recurso usando qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI do ONTAP, o Gerenciador do sistema e a API REST. No entanto, as decisões de autorização e controle de acesso do OAuth 2,0 só podem ser aplicadas quando um cliente acessa o ONTAP usando a API REST.

Os tokens OAuth 2,0 substituem senhas para autenticação de conta de usuário.

Para obter mais informações sobre como usar o OAuth 2,0, consulte "Documentação do ONTAP sobre autenticação e autorização usando OAuth 2,0".

Parâmetros de login e senha

Uma postura de segurança eficaz adere às políticas organizacionais estabelecidas, diretrizes e qualquer governança ou padrões que se apliquem à organização. Exemplos desses requisitos incluem vida útil do nome de usuário, requisitos de comprimento de senha, requisitos de carateres e o armazenamento de tais contas. A solução ONTAP fornece recursos e funções para lidar com essas construções de segurança.

Novos recursos de conta local

Para oferecer suporte às políticas, diretrizes ou padrões de contas de usuário de uma organização, incluindo

governança, a seguinte funcionalidade é suportada no ONTAP:

- Configurando políticas de senha para impor um número mínimo de dígitos, carateres minúsculos ou carateres maiúsculos
- Exigindo um atraso após uma tentativa de login com falha
- Definir o limite inativo da conta
- A expirar uma conta de utilizador
- Exibindo uma mensagem de aviso de expiração de senha
- Notificação de um login inválido

> As configurações configuráveis são gerenciadas usando o comando security login role config modify.

Suporte SHA-512

Para melhorar a segurança da senha, o ONTAP 9 suporta a função hash de senha SHA-2 e usa o padrão SHA-512 para hashing de senhas recém-criadas ou alteradas. Os operadores e administradores também podem expirar ou bloquear contas conforme necessário.

As contas de usuário pré-existentes do ONTAP 9 com senhas inalteradas continuam a usar a função hash MD5 após a atualização para o ONTAP 9.0 ou posterior. No entanto, a NetApp recomenda fortemente que essas contas de usuário migrem para a solução SHA-512 mais segura, fazendo com que os usuários alterem suas senhas.

A funcionalidade hash de senha permite executar as seguintes tarefas:

- Exibir contas de usuário que correspondem à função hash especificada:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- As contas expiram que usam uma função hash especificada (por exemplo, MD5), que força os usuários a alterar suas senhas no próximo login:

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Bloqueie contas com senhas que usam a função hash especificada.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

A função hash de senha é desconhecida para o usuário interno `autosupport` no SVM administrativo do cluster. Esta questão é cosmética. A função hash é desconhecida porque este usuário interno não tem uma senha configurada por padrão.

- Para exibir a função hash de senha para `autosupport` o usuário, execute os seguintes comandos:

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

- Para definir a função hash de senha (padrão: SHA512), execute o seguinte comando:

```
::> security login password -username autosupport
```

  Não importa para que a senha está definida.

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

Parâmetros da palavra-passe

A solução ONTAP suporta parâmetros de senha que atendem e suportam requisitos e diretrizes de políticas organizacionais.

Atributo	Descrição	Padrão	Alcance
`username-minlength`	É necessário um comprimento mínimo do nome de utilizador	3	3-16
`username-alphanum`	Nome de utilizador alfanumérico	desativado	Ativado/desativado
`passwd-minlength`	É necessário um comprimento mínimo da palavra-passe	8	3-64
`passwd-alphanum`	Palavra-passe alfanumérica	ativado	Ativado/desativado
`passwd-min-special-chars`	Número mínimo de carateres especiais necessários na senha	0	0-64
`passwd-expiry-time`	Tempo de expiração da senha (em dias)	Ilimitado, o que significa que as senhas nunca expiram	0-ilimitado 0 expiram agora
`require-initial-passwd-update`	Requer atualização inicial de senha no primeiro login	Desativado	Ativado/desativado Alterações permitidas através de console ou SSH
`max-failed-login-attempts`	Número máximo de tentativas falhadas	0, não bloqueie a conta	-

Atributo	Descrição	Padrão	Alcance
`lockout-duration`	Período máximo de bloqueio (em dias)	O padrão é 0, o que significa que a conta está bloqueada por um dia	-
`disallowed-reuse`	Não permitir as últimas palavras-passe N.	6	O mínimo é 6
`change-delay`	Atraso entre alterações de senha (em dias)	0	-
`delay-after-failed-login`	Atraso após cada tentativa de início de sessão falhada (em segundos)	4	-
`passwd-min-lowercase-chars`	Número mínimo de carateres alfabéticos minúsculos necessário na senha	0, que não requer carateres minúsculos	0-64
`passwd-min-uppercase-chars`	Número mínimo de carateres alfabéticos maiúsculos necessário	0, que não requer carateres maiúsculos	0-64
`passwd-min-digits`	Número mínimo de dígitos necessário na senha	0, que não requer dígitos	0-64
`passwd-expiry-warn-time`	Apresentar mensagem de aviso antes da expiração da palavra-passe (em dias)	Ilimitado, o que significa nunca avisar sobre a expiração da senha	0, o que significa avisar o usuário sobre a expiração da senha após cada login bem-sucedido
`account-expiry-time`	A conta expira em N dias	Ilimitado, o que significa que as contas nunca expiram	O tempo de expiração da conta deve ser maior que o limite inativo da conta
`account-inactive-limit`	Duração máxima de inatividade antes da expiração da conta (em dias)	Ilimitado, o que significa que as contas inativas nunca expiram	O limite inativo da conta deve ser inferior ao tempo de expiração da conta

Exemplo

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

A partir de 9.14.1, há maior complexidade e regras de bloqueio para senhas. Isso se aplica apenas a novas instalações do ONTAP.

Métodos de administração do sistema

Estes são parâmetros importantes para fortalecer a administração do sistema ONTAP.

Acesso à linha de comando

Estabelecer acesso seguro aos sistemas é uma parte essencial da manutenção de uma solução segura. As opções de acesso de linha de comando mais comuns são SSH, Telnet e RSH. Destes, o SSH é a melhor prática mais segura e padrão do setor para acesso remoto à linha de comando. A NetApp recomenda fortemente o uso de SSH para acesso de linha de comando à solução ONTAP.

Configurações SSH

O `security ssh show` comando mostra as configurações dos algoritmos de troca de chaves SSH, cifras e algoritmos MAC para o cluster e SVMs. O método de troca de chaves usa esses algoritmos e cifras para especificar como as chaves de sessão únicas são geradas para criptografia e autenticação e como a autenticação do servidor ocorre.

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

Banners de login

Os banners de login permitem que uma organização apresente quaisquer operadores, administradores e até mesmo errantes com termos e condições de uso aceitável, e eles indicam quem é permitido o acesso ao sistema. Esta abordagem é útil para estabelecer expetativa de acesso e uso do sistema. O `security login banner modify` comando modifica o banner de login. O banner de login é exibido imediatamente antes da etapa de autenticação durante o processo de login do dispositivo SSH e console. O texto do banner deve estar em aspas duplas (" "), como mostrado no exemplo a seguir.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

Parâmetros de banner de login

Parâmetro	Descrição
`vserver`	Use este parâmetro para especificar o SVM com o banner modificado. Use o nome do administrador do cluster SVM para modificar a mensagem no nível do cluster. A mensagem no nível do cluster é usada como padrão para SVMs de dados que não têm uma mensagem definida.

Parâmetro	Descrição
`message`	Este parâmetro opcional pode ser usado para especificar uma mensagem de banner de login. Se o cluster tiver um conjunto de mensagens de banner de login, o banner de login do cluster também será usado por todos os SVMs de dados. A configuração de um banner de login do SVM substitui a exibição do banner de login do cluster. Para redefinir um banner de login SVM de dados para usar o banner de login do cluster, use este parâmetro com o valor "-". Se você usar esse parâmetro, o banner de login não poderá conter novas linhas (também conhecidas como extremidades de linhas [EOLS] ou quebras de linha). Para inserir uma mensagem de banner de login com novas linhas, não especifique nenhum parâmetro. Você é solicitado a inserir a mensagem interativamente. As mensagens inseridas interativamente podem conter novas linhas. Carateres não ASCII devem usar Unicode UTF-8.
`uri`	`(ftp
http):///(hostname	IPv4` Use este parâmetro para especificar o URI a partir do qual o banner de login é baixado. A mensagem não deve exceder 2048 bytes de comprimento. Carateres não ASCII devem ser fornecidos como Unicode UTF-8.

Mensagem do dia

O `security login motd modify` comando atualiza a mensagem do dia (MOTD).

Existem duas categorias de MOTD: O MOTD em nível de cluster e os dados SVM-nível MOTD. Um usuário que faz login no clustershell de um SVM de dados pode ver duas mensagens: O MOTD de nível de cluster seguido pelo MOTD de nível SVM para esse SVM.

O administrador do cluster pode ativar ou desativar o MOTD no nível do cluster em cada SVM individualmente, se necessário. Se o administrador do cluster desativar o MOTD no nível do cluster para um SVM, um usuário que faz login no SVM não verá a mensagem no nível do cluster. Apenas um administrador de cluster pode ativar ou desativar a mensagem de nível de cluster.

Parâmetro MOTD	Descrição
SVM	Use este parâmetro para especificar o SVM para o qual o MOTD é modificado. Use o nome do administrador do cluster SVM para modificar a mensagem no nível do cluster.

Parâmetro MOTD	Descrição
mensagem	Este parâmetro opcional pode ser usado para especificar uma mensagem. Se você usar este parâmetro, o MOTD não pode conter novas linhas. Se você não especificar nenhum parâmetro além do `-vserver` parâmetro, será solicitado que você insira a mensagem interativamente. As mensagens inseridas interativamente podem conter novas linhas. Carateres não ASCII devem ser fornecidos como Unicode UTF-8. A mensagem pode conter conteúdo gerado dinamicamente usando as seguintes sequências de escape: • `\\` - Um único caráter de reação • `\b` - Sem saída (suportado apenas para compatibilidade com Linux) • `\C` - Nome do cluster • `\d` - Data atual como definido no nó de login • `\t` - Hora atual como definido no nó de login • `\I` - Endereço IP de LIF de entrada (imprime console para um `console` login) • `\l` - Nome do dispositivo de login (imprime console para um `console` login) • `\L` - Último login para o usuário em qualquer nó no cluster • `\m` - Arquitetura da máquina • `\n` - Nome do nó ou data SVM • `\N` - Nome do usuário que faz login • `\o` - O mesmo que o. Fornecido para compatibilidade com Linux. • `\O` - Nome de domínio DNS do nó. Observe que a saída depende da configuração da rede e pode estar vazia. • `\r` - Número de versão do software • `\s` - Nome do sistema operacional • `\u` - Número de sessões ativas de clustershell no nó local. Para o administrador do cluster: Todos os usuários do clustershell. Para os dados SVM admin: Apenas sessões ativas para esses dados SVM. • `\U` - Igual a `\u`, mas tem `user` ou `users` anexa • `\v` - String de versão de cluster eficaz • `\W` - Sessões ativas em todo o cluster para o usuário que faz (`who`login)

Para obter mais informações sobre como configurar a mensagem do dia no ONTAP, consulte "Documentação do ONTAP na mensagem do dia".

Tempo limite da sessão da CLI

O tempo limite padrão da sessão da CLI é de 30 minutos. O tempo limite é importante para evitar sessões obsoletas e piggybacking da sessão.

Use o `system timeout show` comando para exibir o tempo limite atual da sessão da CLI. Para definir o

valor de tempo limite, use o `system timeout modify -timeout <minutes>` comando.

Acesso à Web com o Gerenciador do sistema NetApp ONTAP

Se um administrador do ONTAP preferir usar uma interface gráfica em vez da CLI para acessar e gerenciar um cluster, use o Gerenciador do sistema do NetApp ONTAP. Ele é incluído com o ONTAP como um serviço da Web, habilitado por padrão e acessível usando um navegador. Aponte o navegador para o nome do host se estiver usando DNS ou o endereço IPv4 ou IPv6 através `https://cluster-management-LIF`do .

Se o cluster usar um certificado digital autoassinado, o navegador pode exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela autoridade de certificação (CA) no cluster para autenticação do servidor.

A partir do ONTAP 9.3, a autenticação SAML (Security Assertion Markup Language) é uma opção para o Gerenciador de sistemas do ONTAP.

Autenticação SAML para o Gerenciador de sistemas do ONTAP

O SAML 2,0 é um padrão amplamente adotado do setor que permite que qualquer provedor de identidade (IDP) compatível com SAML de terceiros execute MFA usando mecanismos exclusivos para o IDP escolhido pela empresa e como fonte de logon único (SSO).

Há três funções definidas na especificação SAML: O principal, o IDP e o provedor de serviços. Na implementação do ONTAP, um dos principais é o administrador de cluster que obtém acesso ao ONTAP por meio do Gerenciador de sistemas do ONTAP ou do NetApp Active IQ Unified Manager. O IDP é um software IDP de terceiros. A partir do ONTAP 9.3, os Serviços Federados do Microsoft ative Directory (ADFS) e o IDP Shibboleth de código aberto são IDPs suportados. A partir do ONTAP 9.12,1, o Cisco DUO é um IDP suportado. O fornecedor de serviços é a funcionalidade SAML incorporada ao ONTAP usada pelo Gerenciador de sistemas do ONTAP ou pela aplicação Web do Active IQ Unified Manager.

Ao contrário do processo de configuração de dois fatores SSH, depois que a autenticação SAML é ativada, o ONTAP System Manager ou o ONTAP Service Processor Access requer que todos os administradores existentes se autentiquem através do IDP SAML. Não são necessárias alterações nas contas de utilizador do cluster. Quando a autenticação SAML está ativada, um novo método de autenticação de `saml` é adicionado aos usuários existentes com funções de administrador para `http` aplicativos e `ontapi` .

Depois que a autenticação SAML estiver ativada, novas contas adicionais que exigem acesso SAML IDP devem ser definidas no ONTAP com a função de administrador e o método de autenticação saml para `http` aplicativos e `ontapi`. Se a autenticação SAML estiver desativada em algum momento, essas novas contas exigirão que o `password` método de autenticação seja definido com a função de administrador `http` e `ontapi` os aplicativos e a adição `console` do aplicativo para autenticação ONTAP local ao Gerenciador do sistema do ONTAP.

Depois que o IDP SAML é ativado, o IDP executa a autenticação para o acesso do Gerenciador de sistema do ONTAP usando métodos disponíveis para o IDP, como LDAP (Lightweight Directory Access Protocol), AD (ative Directory), Kerberos, senha e assim por diante. Os métodos disponíveis são exclusivos do IDP. É importante que as contas configuradas no ONTAP tenham IDs de usuário mapeadas para os métodos de autenticação IDP.

Os IDPs que foram validados pelo NetApp são Microsoft ADFS, Cisco DUO e IDP de código aberto Shibboleth.

A partir do ONTAP 9.14,1, o Cisco DUO pode ser usado como um segundo fator de autenticação para SSH.

Para obter mais informações sobre o MFA para Gerenciador de sistemas ONTAP, Active IQ Unified Manager e

SSH, "TR-4647: Autenticação multifator no ONTAP 9"consulte .

Insights do Gerenciador de sistemas da ONTAP

A partir do ONTAP 9.11,1, o Gerenciador de sistemas do ONTAP fornece insights para ajudar os administradores de cluster a otimizar suas tarefas diárias. Os insights de segurança são baseados nas recomendações deste relatório técnico.

Insight de segurança	Determinação
O Telnet está ativado	A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro.
O Remote Shell (RSH) está ativado	O NetApp recomenda SSH para acesso remoto seguro.
O AutoSupport está usando um protocolo inseguro	O AutoSupport não está configurado para ser enviado por xref:./ontap-security-hardening/HTTPS.
O banner de login não está configurado no cluster ao nível do cluster	Aviso se o banner de login não estiver configurado para o cluster.
O SSH está usando cifras inseguras	Aviso se o SSH usa cifras inseguras.
Poucos servidores NTP estão configurados	Aviso se o número de servidores NTP configurados for inferior a três.
Usuário de administrador padrão não bloqueado	Quando não estiver usando nenhuma conta administrativa padrão (admin ou diag) para fazer login no System Manager e essas contas não estiverem bloqueadas, a recomendação é bloqueá-las.
Defesa contra ransomware - os volumes não têm políticas Snapshot	Nenhuma política de snapshot adequada é anexada a um ou mais volumes.
Defesa de ransomware - desative a exclusão automática do Snapshot	A eliminação automática de instantâneos está definida para um ou mais volumes.
Os volumes não estão sendo monitorados para ataques de ransomware	A proteção autônoma contra ransomware é suportada em vários volumes, mas ainda não está configurada.
Os SVMs não são configurados para proteção autônoma contra ransomware	A proteção autônoma contra ransomware é suportada em vários SVMs, mas ainda não está configurada.
FPolicy nativo não está configurado	O FPolicy não está definido para SVMs nas.
Ative o modo ativo de proteção autônoma contra ransomware	Vários volumes concluíram o modo de aprendizagem e você pode ativar o modo ativo
A conformidade com o FIPS 140-2 global está desativada	A conformidade com o FIPS 140-2 global não está ativada.
O cluster não está configurado para notificações	E-mails, webhooks ou traphosts SNMP não estão configurados para receber notificações.

Para obter mais informações sobre os insights do Gerenciador de sistemas do ONTAP, consulte "Documentação do ONTAP System Manager Insights".

Proteção autônoma contra ransomware da ONTAP

Para complementar a análise de comportamento do usuário para a segurança de

workloads de workloads de storage, a proteção autônoma contra ransomware do ONTAP analisa workloads de volume e entropia para detectar ransomware e captura Snapshot e notifica o administrador quando houver suspeita de um ataque.

Além da deteção e prevenção de ransomware usando análise comportamental do usuário (UBA) do FPolicy externo com o NetApp Cloud Insights/Cloud Secure e o ecossistema de parceiros do NetApp FPolicy, o ONTAP 9.10,1 introduz proteção autônoma contra ransomware. A proteção autônoma contra ransomware da ONTAP usa uma funcionalidade de aprendizado de máquina (ML) incorporada on-box que analisa a atividade do workload de volume e entropia de dados para detectar automaticamente ransomware. Ele monitora a atividade que é diferente da UBA para que ele possa detetar ataques que a UBA não faz.

Para obter informações mais detalhadas sobre essa capacidade, "Soluções da NetApp para ransomware" consulte ou "Documentação autônoma de proteção de ransomware da ONTAP".

Auditoria de sistema administrativo de storage

Garanta a integridade da auditoria de eventos transferindo eventos do ONTAP para um servidor syslog remoto. Esse servidor pode ser um sistema de gerenciamento de eventos de informações de segurança, como Splunk.

Envie syslog

As informações de log e auditoria são inestimáveis para uma organização do ponto de vista de suporte e disponibilidade. Além disso, as informações e detalhes contidos em logs (syslog) e relatórios de auditoria e saídas são geralmente de natureza sensível. Para manter a postura e os controles de segurança, é imperativo que as organizações gerenciem dados de log e auditoria de maneira segura.

O descarregamento de informações do syslog é necessário para limitar o escopo ou a pegada de uma violação a um único sistema ou solução. Portanto, a NetApp recomenda descarregar com segurança as informações do syslog para um local seguro de armazenamento ou retenção.

Crie um destino de encaminhamento de registos

Use o `cluster log-forwarding create` comando para criar destinos de encaminhamento de log para o log remoto.

Parâmetros

Use os seguintes parâmetros para configurar o `cluster log-forwarding create` comando:

- * Anfitrião de destino.* Esse nome é o nome do host ou o endereço IPv4 ou IPv6 do servidor para o qual encaminhar os logs.

```
-destination <Remote InetAddress>
```

- **Porto de destino.** Esta é a porta na qual o servidor de destino escuta.

```
[-port <integer>]
```

- **Protocolo de encaminhamento de registos.** Este protocolo é utilizado para enviar mensagens para o

destino.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

O protocolo de encaminhamento de registos pode utilizar um dos seguintes valores:

- `udp-unencrypted`. User Datagram Protocol sem segurança.
- `tcp-unencrypted`. TCP sem segurança.
- `tcp-encrypted`. TCP com Transport Layer Security (TLS).

- **Verifique a identidade do servidor de destino.** Quando esse parâmetro é definido como verdadeiro, a identidade do destino de encaminhamento de log é verificada validando seu certificado. O valor só pode ser definido como verdadeiro quando o `tcpencrypted` valor é selecionado no campo protocolo.

```
[-verify-server \{true|false}]
```

- * Syslog facilidade.* Esse valor é o recurso syslog a ser usado para os logs encaminhados.

```
[-facility <Syslog Facility>]
```

- **Ignorar o teste de conetividade.** Normalmente, o `cluster log-forwarding create` comando verifica se o destino está acessível enviando um ping ICMP (Internet Control Message Protocol) e falha se não estiver acessível. Definir este valor para `true` ignorar a verificação de ping para que você possa configurar o destino quando ele não estiver acessível.

```
[-force [true]]
```

O NetApp recomenda usar o `cluster log-forwarding` comando para forçar a conexão a um `-tcp-encrypted` tipo.

Notificação de evento

Proteger as informações e os dados que saem de um sistema é vital para manter e gerenciar a postura de segurança do sistema. Os eventos gerados pela solução ONTAP fornecem uma riqueza de informações sobre o que a solução está encontrando, as informações processadas e muito mais. A vitalidade desses dados destaca a necessidade de gerenciá-los e migrá-los de forma segura.

O `event notification create` comando envia uma nova notificação de um conjunto de eventos definido por um filtro de eventos para um ou mais destinos de notificação. Os exemplos a seguir descrevem a configuração de notificação de eventos e o `event notification show` comando, que exibe os filtros e destinos de notificação de eventos configurados.

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Criptografia de storage

Para proteger dados confidenciais em caso de um disco que seja roubado, devolvido ou reutilizado, use a criptografia de storage NetApp baseada em hardware ou a criptografia de volume NetApp/NetApp agregada baseada em software. Ambos os mecanismos são validados pelo FIPS-140-2 e, ao usar mecanismos baseados em hardware com mecanismos baseados em software, a solução se qualifica para o Programa soluções comerciais para classificados (CSfC). Ele permite maior proteção de segurança para dados secretos e secretos em repouso nas camadas de hardware e software.

A criptografia de dados em repouso é importante para proteger dados confidenciais em caso de um disco que seja roubado, retornado ou reutilizado.

A ONTAP 9 tem três soluções de criptografia de dados em repouso compatíveis com FIPS (Federal Information Processing Standard) 140-2:

- O NetApp Storage Encryption (NSE) é uma solução de hardware que usa unidades com autocriptografia.
- O NetApp volume Encryption (NVE) é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele esteja habilitado com uma chave exclusiva para cada volume.
- O NetApp Aggregate Encryption (NAE) é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele é habilitado com chaves exclusivas para cada agregado.

O NSE, NVE e NAE podem usar o gerenciamento de chaves externas ou o OKM (Onboard Key Manager). O uso de NSE, NVE e NAE não afeta os recursos de eficiência de storage da ONTAP. No entanto, os volumes NVE são excluídos da deduplicação agregada. Os volumes NAE participam e se beneficiam da deduplicação agregada.

O OKM fornece uma solução de criptografia autônoma para dados em repouso com NSE, NVE ou NAE.

NVE, NAE e OKM usam o ONTAP CryptoMod. O CryptoMod está listado na lista de módulos validados do CMVP FIPS 140-2. "FIPS 140-2 Cert no. 4144"Consulte .

Para iniciar a configuração OKM, use o `security key-manager onboard enable` comando. Para configurar gerenciadores de chaves KMIP (Key Management Interoperability Protocol) externos, use o `security key-manager external enable` comando. A partir do ONTAP 9.6, a alocação a vários clientes é suportada para gerentes de chaves externos. Use o `-vserver <vserver name>` parâmetro para habilitar o gerenciamento de chaves externas para uma SVM específica. Antes de 9,6, o `security key-manager setup` comando foi usado para configurar os gerenciadores OKM e de chaves externas. Para o gerenciamento de chaves integradas, essa configuração orienta o operador ou o administrador pela

configuração da senha e parâmetros adicionais para configurar o OKM.

Uma parte da configuração é fornecida no exemplo a seguir:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

A partir do ONTAP 9.4, você pode usar a `-enable-cc-mode` opção True com `security key-manager setup` para exigir que os usuários inseram a senha após uma reinicialização. Para o ONTAP 9.6 e posterior, a sintaxe de comando é `security key-manager onboard enable -cc-mode-enabled yes`.

A partir do ONTAP 9.4, você pode usar o `secure-purge` recurso com privilégios avançados para "esfregar" dados em volumes habilitados para NVE sem interrupções. A análise de dados em um volume criptografado garante que ele não possa ser recuperado da Mídia física. O seguinte comando limpa com segurança os arquivos excluídos no vol1 no SVM VS1:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

A partir do ONTAP 9.7, NAE e NVE são ativados por padrão se a licença VE estiver em vigor, os gerenciadores de chaves externos ou OKM são configurados e NSE não é usado. Os volumes NAE são criados por padrão em agregados NAE e os volumes NVE são criados por padrão em agregados não-naE. Você pode substituir isso digitando o seguinte comando:

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

A partir do ONTAP 9.6, você pode usar um escopo SVM para configurar o gerenciamento de chaves externas para um SVM de dados no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para servir dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário. Para obter mais informações, consulte "Habilite o gerenciamento de chaves externas no ONTAP 9.6 e posterior" a documentação do ONTAP.

A partir do ONTAP 9.11,1, é possível configurar a conetividade com servidores de gerenciamento de chaves externas em cluster, designando servidores de chaves primárias e secundárias em um SVM. Para obter mais informações, consulte "configurar servidores de chaves externas em cluster" a documentação do ONTAP.

A partir do ONTAP 9.13,1, você pode configurar servidores de gerenciador de chaves externos no gerenciador de sistema. Para obter mais informações, consulte "Gerenciar gerenciadores de chaves externos" a documentação do ONTAP.

Criptografia de replicação de dados

Para complementar os dados em repouso, é possível criptografar o tráfego de replicação de dados do ONTAP entre clusters usando o TLS 1,2 com uma chave pré-compartilhada para SnapMirror, SnapVault ou FlexCache.

Ao replicar dados para recuperação de desastre, armazenamento em cache ou backup, você precisa proteger esses dados durante o transporte por cabo de um cluster ONTAP para outro. Isso evita ataques intermediários maliciosos contra dados confidenciais quando eles estão em trânsito.

A partir do ONTAP 9.6, a criptografia de peering de cluster fornece suporte de criptografia TLS 1,2 AES-256 GCM para recursos de replicação de dados do ONTAP, como SnapMirror, SnapVault e FlexCache. A criptografia é configurada por meio de uma chave pré-compartilhada (PSK) entre dois pares de cluster.

Clientes que usam tecnologias como NSE, NVE e NAE para proteger dados em repouso também podem usar criptografia de dados completa atualizando para o ONTAP 9.6 ou posterior para usar a criptografia de peering de cluster.

O peering de cluster criptografa todos os dados entre os pares do cluster. Por exemplo, ao usar o SnapMirror, todas as informações de peering, bem como todas as relações SnapMirror entre o peer de cluster de origem e destino são criptografadas. Não é possível enviar dados de texto não criptografado entre pares de cluster com criptografia de peering de cluster ativada.

A partir do ONTAP 9.6, as novas relações de cluster-peer têm a encriptação ativada por predefinição. Para habilitar a criptografia em relacionamentos de pares de cluster que foram criados antes do ONTAP 9.6, você deve atualizar o cluster de origem e destino para 9,6. Além disso, você deve usar o `cluster peer modify` comando para alterar os pares de cluster de origem e destino para usar a criptografia de peering de cluster.

Você pode converter um relacionamento de pares existente para usar a criptografia de peering de cluster no ONTAP 9.6, conforme mostrado no exemplo a seguir:

```
On the Destination Cluster Peer

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the Source Cluster Peer

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

Criptografia de dados em trânsito IPsec

Os clientes que usam tecnologias de criptografia de dados em repouso, como criptografia de storage NetApp (NSE) ou criptografia de volume NetApp (NVE) e criptografia de peering de cluster (CPE) para tráfego de replicação de dados, agora podem usar criptografia de ponta a ponta entre o cliente e o storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9 ou posterior e usando IPsec. O IPsec fornece uma alternativa à criptografia NFS ou SMB/CIFS e é a única opção de criptografia em voo para tráfego iSCSI.

Em algumas situações, pode haver um requisito para proteger todos os dados do cliente transportados por cabo (ou em trânsito) para o SVM do ONTAP. Isso impede a repetição e ataques maliciosos contra dados confidenciais em trânsito.

A partir do ONTAP 9.8, a Segurança de Protocolo de Internet (IPsec) oferece suporte de criptografia de ponta a ponta para todo o tráfego IP entre um cliente e um SVM do ONTAP. A criptografia de dados IPsec para todo o tráfego IP inclui protocolos NFS, iSCSI e SMB/CIFS. O IPsec fornece a única opção de criptografia em voo para tráfego iSCSI.

Fornecer criptografia NFS por cabo é um dos principais casos de uso do IPsec. Antes do ONTAP 9.8, a criptografia por cabo NFS exigiu a configuração e configuração do Kerberos para utilizar o krb5p para criptografar dados NFS em trânsito. Isso nem sempre é simples ou fácil de realizar em todos os ambientes do cliente.

Os clientes que usam tecnologias de criptografia de dados em repouso, como criptografia de storage NetApp (NSE) ou criptografia de volume NetApp (NVE) e criptografia de peering de cluster (CPE) para tráfego de replicação de dados, agora podem usar criptografia de ponta a ponta entre o cliente e o storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9 ou posterior e usando IPsec.

IPsec é um padrão IETF. O ONTAP usa IPsec no modo de transporte. Ele também aproveita o protocolo IKE (Internet Key Exchange) versão 2, que usa uma chave pré-compartilhada (PSK) para negociar material chave entre o cliente e o ONTAP com IPv4 ou IPv6. Por padrão, o IPsec usa criptografia de 256 bits AES-GCM do Suite-B. Suite-B AES-GMAC256 e AES-CBC256 com encriptação de 256 bits também são suportados.

Embora o recurso IPsec deva estar habilitado no cluster, ele se aplica a endereços IP SVM individuais por

meio do uso de uma entrada SPD (Security Policy Database). A entrada SPD (diretiva) contém o endereço IP do cliente (sub-rede IP remota), o endereço IP SVM (sub-rede IP local), o conjunto de codificação de criptografia a ser usado e o segredo pré-compartilhado (PSK) necessário para autenticar via IKEv2 e estabelecer a conexão IPsec. Além da entrada de diretiva IPsec, o cliente deve ser configurado com as mesmas informações (IP local e remoto, PSK e conjunto de codificação) antes que o tráfego possa fluir pela conexão IPsec. A partir do ONTAP 9.10,1, o suporte à autenticação de certificado IPsec é adicionado. Isso remove os limites de diretiva IPsec e habilita o suporte do sistema operacional Windows para IPsec.

Se houver um firewall entre o cliente e o endereço IP SVM, ele deverá permitir que os protocolos ESP e UDP (portas 500 e 4500), tanto de entrada (entrada) quanto de saída (saída), para que a negociação IKEv2 seja bem-sucedida e, assim, permita o tráfego IPsec.

Para criptografia de tráfego de peering de cluster e NetApp SnapMirror, a criptografia de peering de cluster (CPE) ainda é recomendada por IPsec para garantir o trânsito seguro por cabo. O CPE tem melhor desempenho para essas cargas de trabalho do que o IPsec. Você não precisa de uma licença para IPsec e não há restrições de importação ou exportação.

Você pode ativar o IPsec no cluster e criar uma entrada SPD para um único cliente e um único endereço IP SVM, conforme mostrado no exemplo a seguir:

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

Modo FIPS e gerenciamento TLS e SSL

O padrão FIPS 140-2 especifica requisitos de segurança para módulos criptográficos dentro de sistemas de segurança que protegem informações confidenciais em sistemas de computador e telecomunicações. O padrão FIPS 140-2 aplica-se *especificamente* ao módulo criptográfico, em vez do produto, arquitetura, dados ou ecossistema. O módulo criptográfico é o componente específico (hardware, software, firmware ou uma combinação dos três) que implementa funções de segurança aprovadas pelo NIST.

A ativação da conformidade com o FIPS 140-2 tem efeitos em outros sistemas e comunicações internas e externas ao ONTAP 9. A NetApp recomenda fortemente testar essas configurações em um sistema que não seja de produção com acesso ao console.

A partir do suporte a ONTAP 9.11,1 e TLS 1,3, é possível validar o FIPS 140-3.

A configuração FIPS se aplica ao ONTAP e ao Platform BMC.

Configuração do modo FIPS do NetApp ONTAP

O NetApp ONTAP tem uma configuração do modo FIPS que instancia um nível adicional de segurança ao plano de controle:

- A partir do ONTAP 9.11,1, quando o modo de conformidade com o FIPS 140-2 estiver ativado, TLSv1, TLSv1,1 e SSLv3 serão desativados e apenas TSLv1,2 e TSLv1,3 permanecerão ativados. Afeta outros sistemas e comunicações que são internos e externos ao ONTAP 9. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativar, TLSv1, TLSv1,1 e SSLv3 permanecerão desativados. O TLSv1,2 ou o TLSv1,3 permanecerão ativados dependendo da configuração anterior.
- Para versões do ONTAP anteriores a 9.11.1, quando o modo de conformidade com FIPS 140-2 estiver ativado, tanto o TLSv1 quanto o SSLv3 são desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando o modo de conformidade FIPS 140-2 estiver ativado. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativá-lo, o TLSv1 e o SSLv3 permanecerão desativados, mas o TLSv1,2 ou o TLSv1,1 e o TLSv1,2 serão ativados dependendo da configuração anterior.
- "Módulo de segurança criptográfica NetApp (NCSM)", Validado pelo FIPS 140-2 nível 1, fornece conformidade com software.

> O NIST enviou um padrão FIPS-140-3 e o NCSM terá validações FIPS-140-2 e FIPS-140-3. Todas as validações do FIPS 140-2 serão transferidas para o status histórico em 21 de setembro de 2026, ou seja, cinco anos após o último dia para novos envios de certificados.

Ative o modo de conformidade FIPS-140-2 e FIPS-140-3

A partir do ONTAP 9, é possível habilitar o modo de conformidade FIPS-140-2 e FIPS-140-3 para interfaces do plano de controle em todo o cluster.

- "Ativar FIPS"
- "Exibir status FIPS"

Protocolos e capacitação FIPS

O `security config modify` comando permite modificar a configuração de segurança existente em todo o cluster. Se ativar o modo compatível com FIPS, o cluster selecionará automaticamente apenas protocolos TLS.

- Use o `-supported-protocols` parâmetro para incluir ou excluir protocolos TLS independentemente do modo FIPS. Por padrão, o modo FIPS é desativado e o ONTAP oferece suporte aos protocolos TLSv1,2, TLSv1,1 e TLSv1.
- Para compatibilidade com versões anteriores, o ONTAP suporta a adição de SSLv3 à lista de protocolos compatíveis quando o modo FIPS está desativado.

Capacitação FIPS e cifras

- Utilize o `-supported-cipher-suites` parâmetro para configurar apenas o AES (Advanced Encryption Standard) ou AES e 3DES.
- Você pode desativar cifras fracas, como RC4, especificando `!RC4`. Por padrão, a configuração de codificação suportada é `ALL:!LOW:!aNULL:!EXP:!eNULL`. Essa configuração significa que todos os conjuntos de criptografia suportados para os protocolos estão ativados, exceto aqueles que usam algoritmos de criptografia de 64 bits ou 56 bits sem autenticação, criptografia, sem exportação e pacotes de criptografia de baixa criptografia.
- Selecione um conjunto de codificações que esteja disponível com o protocolo selecionado correspondente. Uma configuração inválida pode fazer com que algumas funcionalidades não funcionem corretamente.

- Para obter a sintaxe correta da cadeia de carateres de cifra, consulte "página de cifras" On OpenSSL (publicado pela fundação do software OpenSSL). A partir do ONTAP 9.9,1 e versões posteriores, não é mais necessário reiniciar todos os nós manualmente depois de modificar a configuração de segurança.

Proteção de segurança SSH e TLS

A administração SSH do ONTAP 9 requer um cliente OpenSSH 5,7 ou posterior. Os clientes SSH devem negociar com o algoritmo de chave pública ECDSA (Elliptic Curve Digital Signature Algorithm) para que a conexão seja bem-sucedida.

Para proteger a segurança TLS, ative apenas o TLS 1,2 e use conjuntos de codificação capazes de Perfect Forward Secrecy (PFS). O PFS é um método de troca de chaves que, quando usado em combinação com protocolos de criptografia como o TLS 1,2, ajuda a impedir que um invasor descriptografe todas as sessões de rede entre um cliente e um servidor.

Ative os conjuntos de codificação compatíveis com TLSv1,2 e PFS

Para ativar apenas conjuntos de encriptação compatíveis com TLS 1,2 e PFS, utilize o `security config modify` comando a partir do nível de privilégio avançado.

Antes de alterar a configuração da interface SSL, certifique-se de que o cliente suporta as cifras DHE e ECDHE ao se conetar ao ONTAP para manter a conetividade com o ONTAP.

Exemplo

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirme `y` para cada prompt. Para obter mais informações sobre PFS, consulte este "NetApp blog".

Informações relacionadas

"Publicação Federal Information Processing Standard (FIPS) 140"

Crie um certificado digital assinado pela CA

Para muitas organizações, o certificado digital auto-assinado para o acesso à Web ONTAP não é compatível com suas políticas INFOSEC. Em sistemas de produção, é uma prática recomendada do NetApp instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou SVM como um servidor SSL.

Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR) e o `security certificate install` comando para instalar o certificado recebido de volta da CA.

Passos

1. Para criar um certificado digital assinado pela CA da organização, faça o seguinte:
   a. Gerar um CSR.
   b. Siga o procedimento da sua organização para solicitar um certificado digital usando a CSR da CA da sua organização. Por exemplo, usando a interface da Web do Microsoft ative Directory Certificate

Services, vá para `<CA_server_name>/certsrv` e solicite um certificado.

c. Instale o certificado digital no ONTAP.

Protocolo de estado do certificado online

O OCSP (Online Certificate Status Protocol) permite que aplicativos ONTAP que usam comunicações TLS, como LDAP ou TLS, recebam status de certificado digital quando o OCSP está ativado. O aplicativo recebe uma resposta assinada significando que o certificado solicitado é bom, revogado ou desconhecido.

O OCSP permite determinar o status atual de um certificado digital sem exigir listas de revogação de certificados (CRLs).

Por padrão, a verificação do status do certificado OCSP está desativada. Ele pode ser ativado com o comando `security config ocsp enable -app name`, onde o nome do aplicativo pode ser `autosupport`, `audit_log`, `fabricpool` `ems` , , , `kmip`, `ldap_ad`, `ldap_nis_namemap`, `all` ou . O comando requer nível de privilégio avançado.

Gerenciamento do SSHv2

O `security ssh modify` comando substitui as configurações existentes dos algoritmos de troca de chaves SSH, cifras ou algoritmos MAC para o cluster ou um SVM com as configurações especificadas.

A NetApp recomenda o seguinte:

- Use senhas para sessões de usuário.
- Use uma chave pública para acesso à máquina.

Cifras suportadas e trocas de chaves

Cifras	Troca de chaves
aes256-ctr	diffie-hellman-group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-group-Exchange-SHA1 (SHA-1)
aes128-ctr	diffie-hellman-group14-SHA1 (SHA-1)
aes256-cbc	diffie-hellman-group1-SHA1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Criptografia simétrica AES e 3DES suportada

O ONTAP também suporta os seguintes tipos de criptografia simétrica AES e 3DES (também conhecidos como cifras):

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm

A configuração de gerenciamento SSH se aplica ao ONTAP e à plataforma BMC.

NetApp AutoSupport

O recurso AutoSupport do ONTAP permite que você monitore proativamente a integridade do sistema e envie mensagens e detalhes automaticamente para o suporte técnico da NetApp, para a equipe de suporte interna da organização ou para um parceiro de suporte. Por padrão, as mensagens AutoSupport para o suporte técnico do NetApp são ativadas quando o sistema de armazenamento é configurado pela primeira vez. Além disso, o AutoSupport começa a enviar mensagens para o suporte técnico da NetApp 24 horas depois de ativado. Este período de 24 horas é configurável. Para aproveitar a comunicação com a equipe de suporte interno de uma organização, a configuração do host de e-mail deve ser concluída.

Somente o administrador do cluster pode executar o gerenciamento de AutoSupport (configuração). O administrador do SVM não tem acesso ao AutoSupport. O recurso AutoSupport pode ser desativado. No entanto, a NetApp recomenda habilitá-la porque o AutoSupport ajuda a acelerar a identificação e a resolução de problemas caso ocorra algum problema no sistema de storage. Por padrão, o sistema coleta informações do AutoSupport e as armazena localmente, mesmo que você desative o AutoSupport.

Para obter mais detalhes sobre mensagens AutoSupport, incluindo o que está contido nas várias mensagens e onde diferentes tipos de mensagens são enviadas, consulte "Consultor digital da NetApp"a documentação.

As mensagens do AutoSupport contêm dados confidenciais, incluindo, entre outros, os seguintes itens:

- Ficheiros de registo
- Dados sensíveis ao contexto relativos a subsistemas específicos
- Dados de configuração e status
- Dados de performance

O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível das mensagens AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens AutoSupport para o suporte ao NetApp.

Além disso, você deve utilizar o `system node autosupport modify` comando para especificar os destinos dos dados do AutoSupport (por exemplo, suporte técnico da NetApp, operações internas de uma organização ou parceiros). Esse comando também permite especificar quais detalhes específicos do AutoSupport enviar (por exemplo, dados de desempenho, arquivos de log, etc.).

Para desativar completamente o AutoSupport, use o `system node autosupport modify -state disable` comando.

Protocolo de hora de rede

Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster com pelo menos três servidores NTP externos.

Podem ocorrer problemas quando o tempo do cluster é impreciso. Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster com servidores NTP externos.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Você pode associar um máximo de 10 servidores NTP externos usando o `cluster time-service ntp server create` comando. Para redundância e qualidade do serviço de tempo, você deve associar pelo menos três servidores NTP externos ao cluster.

Para obter detalhes sobre a configuração do NTP no ONTAP, "Gerenciamento do tempo do cluster (somente administradores de cluster)"consulte .

Contas locais do sistema de arquivos nas (grupo de trabalho CIFS)

A autenticação de cliente de grupo de trabalho fornece uma camada extra de segurança para a solução ONTAP que é consistente com uma postura tradicional de autenticação de domínio. Use o `vserver cifs session show` comando para exibir vários detalhes relacionados à postura, incluindo informações IP, mecanismo de autenticação, versão do protocolo e tipo de autenticação.

A partir do ONTAP 9, você pode configurar um servidor CIFS em um grupo de trabalho com clientes CIFS que se autenticam no servidor usando usuários e grupos definidos localmente. A autenticação de cliente de grupo

de trabalho fornece uma camada extra de segurança para a solução ONTAP que é consistente com uma postura tradicional de autenticação de domínio. Para configurar o servidor CIFS, use o `vserver cifs create` comando. Depois que o servidor CIFS é criado, você pode associá-lo a um domínio CIFS ou associá-lo a um grupo de trabalho. Para ingressar em um grupo de trabalho, use o `-workgroup` parâmetro. Aqui está um exemplo de configuração:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

Um servidor CIFS no modo de grupo de trabalho suporta apenas a autenticação do Windows NT LAN Manager (NTLM) e não suporta autenticação Kerberos.

A NetApp recomenda a utilização da função de autenticação NTLM com grupos de trabalho CIFS para manter a postura de segurança da sua organização. Para validar a postura de segurança do CIFS, o NetApp recomenda o uso do `vserver cifs session show` comando para exibir vários detalhes relacionados à postura, incluindo informações de IP, mecanismo de autenticação, versão do protocolo e tipo de autenticação.

Auditoria do sistema de arquivos nas

Os sistemas de arquivos nas ocupam um espaço maior no cenário de ameaças atuais. As funções de auditoria são essenciais para oferecer suporte à visibilidade.

A segurança requer validação. O ONTAP 9 fornece maiores eventos de auditoria e detalhes em toda a solução. Como os sistemas de arquivos nas ocupam um espaço físico maior no cenário de ameaças atuais, as funções de auditoria são essenciais para oferecer suporte à visibilidade. Devido à capacidade de auditoria aprimorada no ONTAP 9, os detalhes de auditoria do CIFS são mais abundantes do que nunca. Os principais detalhes, incluindo os seguintes, são registrados com eventos criados:

- Acesso a arquivos, pastas e compartilhamentos
- Arquivos criados, modificados ou excluídos
- Acesso de leitura de ficheiros bem-sucedido
- Tentativas falhadas de ler ou gravar ficheiros
- Alterações de permissão de pasta

Crie uma configuração de auditoria

É necessário habilitar a auditoria CIFS para gerar eventos de auditoria. Use o `vserver audit create` comando para criar uma configuração de auditoria. Por padrão, o log de auditoria usa um método de rotação baseado no tamanho. Você pode usar uma opção de rotação baseada no tempo, se especificado no campo Rotation Parameters (parâmetros de rotação). Os detalhes adicionais da configuração de rotação de auditoria de log incluem o cronograma de rotação, os limites de rotação, os dias de rotação da semana e o tamanho da rotação. O texto a seguir fornece um exemplo de configuração que descreve uma configuração de auditoria usando uma rotação mensal baseada em tempo agendada para todos os dias da semana às 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Eventos de auditoria CIFS

Os eventos de auditoria CIFS são os seguintes:

- **Compartilhamento de arquivos**: Gera um evento de auditoria quando um compartilhamento de rede CIFS é adicionado, modificado ou excluído usando os comandos relacionados `vserver cifs share`.
- **Alteração da política de auditoria**: Gera um evento de auditoria quando a política de auditoria é desativada, ativada ou modificada usando os comandos relacionados `vserver audit`.
- **Conta de usuário**: Gera um evento de auditoria quando um usuário local CIFS ou UNIX é criado ou excluído; uma conta de usuário local é ativada, desativada ou modificada; ou uma senha é redefinida ou alterada. Este evento usa o `vserver cifs users-and-groups local-group` comando ou o comando relacionado `vserver services name-service unix-user`.
- **Security group**: Gera um evento de auditoria quando um grupo de segurança local CIFS ou UNIX é criado ou excluído usando o `vserver cifs users-and-groups local-group` comando ou o comando relacionado `vserver services name-service unix-group`.
- **Alteração da política de autorização**: Gera um evento de auditoria quando os direitos são concedidos ou revogados para um usuário CIFS ou um grupo CIFS usando o `vserver cifs users-and-groups privilege` comando.

> Esta funcionalidade é baseada na função de auditoria do sistema, que permite que um administrador analise o que o sistema está permitindo e executando a partir da perspetiva de um usuário de dados.

Efeito de APIS REST na auditoria nas

O ONTAP inclui a capacidade de contas de administrador acessarem e manipularem arquivos SMB/CIFS ou NFS usando APIs REST. Embora as APIS REST só possam ser executadas por administradores do ONTAP, os comandos da API REST ignoram o log de auditoria nas do sistema. Além disso, as permissões de arquivo também podem ser ignoradas pelos administradores do ONTAP ao usar APIs REST. No entanto, as ações do administrador com APIs REST em arquivos são capturadas no log do histórico de comandos do sistema.

Criar função de API REST sem acesso

É possível impedir que os administradores do ONTAP usem APIS REST para acesso a arquivos ao criar uma função de API REST que não tenha acesso a volumes do ONTAP por meio DE REST. Para provisionar essa função, execute as etapas a seguir.

Passos

1. Crie uma nova função REST que não tenha acesso a volumes de storage, além de ter todos os outros acessos à API REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Atribua a conta de administrador à nova função API REST que você criou na etapa anterior.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

Se você quiser impedir que a conta de administrador de cluster do ONTAP integrada use APIS REST para acesso a arquivos, primeiro será necessário "crie uma nova conta de administrador e desative ou exclua a conta interna".

Configure e ative a assinatura e a vedação CIFS SMB

Você pode configurar e ativar a assinatura SMB que protege a segurança do Data Fabric. Isso garante que o tráfego entre sistemas de storage e clientes não seja comprometido com replay ou ataques man-in-the-middle. A assinatura SMB protege verificando se as mensagens SMB têm assinaturas válidas.

Sobre esta tarefa

Um vetor de ameaça comum para sistemas de arquivos e arquiteturas está no protocolo SMB. Para lidar com esse vetor, a solução ONTAP 9 usa assinatura e vedação padrão do setor SMB. A assinatura de SMB protege a segurança do Data Fabric ao garantir que o tráfego entre sistemas de storage e clientes não seja comprometido com replays ou ataques diretos. Ele faz isso verificando se as mensagens SMB têm assinaturas válidas.

Embora a assinatura SMB esteja desativada por padrão no interesse do desempenho, a NetApp recomenda fortemente que você a ative. Além disso, a solução ONTAP oferece suporte à criptografia SMB, que também é conhecida como vedação. Esta abordagem permite o transporte seguro de dados numa base de partilha por partilha. Por predefinição, a encriptação SMB está desativada. No entanto, a NetApp recomenda que você ative a criptografia SMB.

Agora, a assinatura e a vedação LDAP são suportadas no SMB 2,0 e posterior. A assinatura (proteção contra adulteração) e a vedação (criptografia) permitem a comunicação segura entre SVMs e servidores do ative Directory. A criptografia AES acelerada (Intel AES NI) agora é suportada no SMB 3,0 e posterior. O Intel AES NI melhora o algoritmo AES e acelera a criptografia de dados com famílias de processadores suportadas.

Passos

1. Para configurar e ativar a assinatura SMB, use o `vserver cifs security modify` comando e verifique se o `-is-signing-required` parâmetro está definido como `true`. Veja o seguinte exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Para configurar e ativar a selagem e a criptografia SMB, use o `vserver cifs security modify` comando e verifique se o `-is-smb-encryption-required` parâmetro está definido como `true`. Veja o seguinte exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Proteção do NFS

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente para um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente. Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação.

O controle de acesso é fundamental para manter uma postura segura. Portanto, o ONTAP usa o recurso de política de exportação para limitar o acesso de volume NFS a clientes que correspondem a parâmetros específicos. As políticas de exportação contêm uma ou mais regras de exportação que processam cada solicitação de acesso de cliente. Uma política de exportação está associada a cada volume para configurar o acesso do cliente ao volume. O resultado deste processo determina se o cliente é concedido ou negado (com uma mensagem de permissão negada) o acesso ao volume. Este processo também determina que nível de acesso é fornecido ao volume.

Uma política de exportação com regras de exportação deve existir em um SVM para que os clientes acessem os dados. Um SVM pode conter várias políticas de exportação.

A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

As regras de exportação determinam as permissões de acesso do cliente aplicando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação (por exemplo, NFSv4 ou SMB)
- Um identificador de cliente (por exemplo, nome de host ou endereço IP)
- O tipo de segurança usado pelo cliente para autenticar (por exemplo, Kerberos v5, NTLM ou AUTH_SYS)

Se uma regra especificar vários critérios e o cliente não corresponder a um ou mais deles, a regra não se aplica.

Um exemplo de política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

O tipo de segurança determina o nível de acesso que um cliente recebe. Os três níveis de acesso são somente leitura, leitura-gravação e superusuário (para clientes com ID de usuário `0`). Como o nível de acesso determinado pelo tipo de segurança é avaliado nesta ordem, você deve observar as regras listadas:

Regras para parâmetros de nível de acesso em regras de exportação

Para que um cliente obtenha os seguintes níveis de acesso	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente
Apenas de leitura normal do utilizador	Somente leitura (`-rorule`)
Leitura-escrita normal do utilizador	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`)
Somente leitura do superusuário	Apenas leitura (`-rorule`) e. `-superuser`
Leitura-gravação do superusuário	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`) e. `-superuser`

Os seguintes são tipos de segurança válidos para cada um destes três parâmetros de acesso:

- Qualquer
- Nenhum
- Nunca

Esses tipos de segurança não são válidos para uso com o `-superuser` parâmetro:

- krb5
- ntlm
- sistema

Regras para resultados de parâmetros de acesso

Se o tipo de segurança do cliente …	Então …
Corresponde a um tipo de segurança especificado no parâmetro de acesso.	O cliente recebe acesso para esse nível com seu próprio ID de usuário.
Não corresponde a um tipo de segurança especificado, mas o parâmetro Access inclui a opção `none`.	O cliente recebe acesso para esse nível e recebe o usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro.

Se o tipo de segurança do cliente …	Então …
Não corresponde a um tipo de segurança especificado e o parâmetro Access não inclui a opção `none`.	O cliente não recebe nenhum acesso para esse nível. Esta restrição não se aplica ao `-superuser` parâmetro porque este parâmetro sempre inclui nenhum, mesmo quando não especificado.

Kerberos 5 e Krb5p

A partir do ONTAP 9, a autenticação Kerberos 5 com serviço de privacidade (krb5p) é suportada. O modo de autenticação krbp5 é seguro e protege contra adulteração e espionagem de dados usando checksums para criptografar todo o tráfego entre cliente e servidor. A solução ONTAP suporta criptografia AES de 128 bits e 256 bits para Kerberos. O serviço de privacidade inclui verificar a integridade dos dados recebidos, autenticar usuários e criptografar dados antes da transmissão.

A opção krb5p está mais presente no recurso de política de exportação, onde é definida como uma opção de criptografia. O método de autenticação krb5p.1X pode ser usado como um parâmetro de autenticação, como mostrado no exemplo a seguir:

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Ative a assinatura e a vedação do protocolo Lightweight Directory Access

Assinatura e selagem são suportados para habilitar a segurança da sessão em consultas a um servidor LDAP. Essa abordagem fornece uma alternativa à segurança de sessão LDAP-over-TLS.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. As configurações de segurança de sessão em um SVM correspondem às disponíveis no servidor LDAP. Por padrão, a assinatura e a vedação LDAP são desativadas.

Passos

1. Para ativar esta função, execute o `vserver cifs security modify` comando com o `session-security-for-ad-ldap` parâmetro.

   Opções para funções de segurança LDAP:

   - **Nenhum**: Padrão, sem assinatura ou vedação
   - **Sign**: Assine o tráfego LDAP
   - **Seal**: Assine e criptografe o tráfego LDAP

Os parâmetros de sinal e selo são cumulativos, o que significa que, se a opção de sinal for usada, o resultado será LDAP com assinatura. No entanto, se a opção de vedação for usada, o resultado será sinal e selo. Além disso, se um parâmetro não for especificado para esse comando, o padrão será nenhum.

O seguinte é um exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Crie e use um FPolicy do NetApp

Você pode criar e usar um FPolicy, um componente de infraestrutura da solução ONTAP, que permite que aplicativos parceiros monitorem e definam permissões de acesso a arquivos. Uma das aplicações mais avançadas é a Segurança de workload de storage, uma aplicação SaaS da NetApp que oferece visibilidade e controle centralizados de todos os acessos a dados corporativos em ambientes de nuvem híbrida para garantir que as metas de segurança e conformidade sejam atingidas.

O controle de acesso é um conceito chave de segurança. A visibilidade e a capacidade de responder a acesso aos arquivos e operações de arquivos são essenciais para manter sua postura de segurança. Para fornecer visibilidade e controle de acesso para arquivos, a solução ONTAP usa o recurso NetApp FPolicy.

As políticas de arquivo podem ser definidas com base no tipo de arquivo. O FPolicy determina como o sistema de armazenamento processa solicitações de sistemas clientes individuais para operações como criar, abrir, renomear e excluir. A partir do ONTAP 9, a estrutura de notificação de acesso a arquivos FPolicy é aprimorada com controles de filtragem e resiliência contra interrupções de rede curtas.

Passos

1. Para aproveitar o recurso FPolicy, primeiro você deve criar a política FPolicy com o `vserver fpolicy policy create` comando.

   Além disso, use o `-events` parâmetro se você usar o FPolicy para visibilidade e a coleção de eventos. A granularidade adicional fornecida pelo ONTAP permite filtrar e acessar o nível de controle do nome de usuário. Para controlar o Privileges e o acesso com nomes de usuário, especifique o `-privilege-user-name` parâmetro.

   O texto a seguir fornece um exemplo de criação de FPolicy:

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. Depois de criar a política FPolicy, você deve ativá-la com o `vserver fpolicy enable` comando. Este comando também define a prioridade ou a sequência da entrada FPolicy.

A sequência FPolicy é importante porque, se várias políticas se inscreveram no mesmo evento de acesso ao arquivo, a sequência dita a ordem em que o acesso é concedido ou negado.

O texto a seguir fornece uma configuração de exemplo para ativar a política FPolicy e validar a configuração com o `vserver fpolicy show` comando:

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                     Sequence  Status
Engine
----------------------- ------------------------------ --------  -------
-------
vs1.example.com         vs1_pol
vs2.example.com         vs2_pol
 external
2 entries were displayed.
```

Melhorias de FPolicy

O ONTAP 9 inclui os aprimoramentos de FPolicy descritos nas seções a seguir.

Controlos de filtragem

Novos filtros estão disponíveis para `SetAttr` e para remover notificações sobre atividades de diretório.

Resiliência assíncrona

Se um servidor FPolicy que opera no modo assíncrono sofrer uma interrupção na rede, as notificações FPolicy geradas durante a interrupção serão armazenadas no nó de storage. Quando o servidor FPolicy volta online, ele é alertado das notificações armazenadas e pode buscá-las a partir do nó de armazenamento. O período de tempo em que as notificações podem ser armazenadas durante uma interrupção é configurável até 10 minutos.

Segurança LIF

Um LIF é um endereço IP ou nome de porta mundial (WWPN) com caraterísticas associadas, como uma função, uma porta inicial, um nó inicial, uma lista de portas para failover e uma política de firewall. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede. É fundamental entender as caraterísticas de segurança de cada função de LIF.

Funções do LIF

As funções de LIF podem ser as seguintes:

- **Data LIF**: Um LIF associado a um SVM e usado para comunicação com clientes.
- **Cluster LIF**: Um LIF usado para transportar tráfego entre nós em um cluster.
- **LIF de gerenciamento de nós**: Um LIF que fornece um endereço IP dedicado para gerenciar um nó específico em um cluster.
- **Cluster Management LIF**: Um LIF que fornece uma única interface de gerenciamento para todo o cluster.
- **Intercluster LIF**: Um LIF usado para comunicação entre clusters, backup e replicação.

Caraterísticas de segurança de cada função de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Requer sub-rede IP privada?	Não	Sim	Não	Não	Não
Requer rede segura?	Não	Sim	Não	Não	Sim
Política de firewall predefinida	Muito restritivo	Completamente aberto	Média	Média	Muito restritivo
O firewall é personalizável?	Sim	Não	Sim	Sim	Sim

- Como o LIF do cluster está completamente aberto sem política de firewall configurável, ele deve estar em uma sub-rede IP privada em uma rede segura isolada.
- Sob nenhuma circunstância quaisquer papéis de LIF devem ser expostos à Internet.

Saiba mais sobre como proteger LIFs, consulte "Configurar políticas de firewall para LIFs".

Segurança de protocolo e porta

Além de executar operações e funções de segurança on-box, o endurecimento de uma solução também deve incluir mecanismos de segurança off-box. Aproveitar dispositivos de infraestrutura adicionais, como firewalls, sistemas de prevenção de intrusão (IPSs) e outros dispositivos de segurança, para filtrar e limitar o acesso ao ONTAP é uma maneira eficaz de estabelecer e manter uma postura de segurança rigorosa. Esta informação é um componente chave para filtrar e limitar o acesso ao ambiente e aos seus recursos.

Protocolos e portas comumente usados

Serviço	Porta/protocolo	Descrição
`SSH`	22/TCP	Login SSH
`telnet`	23/TCP	Início de sessão remoto
`Domain`	53/TCP	Servidor de nomes de domínio

Serviço	Porta/protocolo	Descrição
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	Chamada de procedimento remoto
NTP	123/UDP	Protocolo de hora de rede
msrpc	135/UDP	Chamada de procedimento remoto da Microsoft
Netbios-name	137/TCP 137/UDP	Serviço de nomes NetBIOS
netbios-ssn	139/TCP	Sessão de serviço NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Link seguro:http
microsoft-ds	445/TCP	Serviços de diretório Microsoft
IPsec	500/UDP	Segurança do protocolo da Internet
mount	635/UDP	Montagem em NFS
named	953/UDP	Daemon de nomes
NFS	2049/UDP 2049/TCP	Daemon do servidor NFS
nrv	2050/TCP	Protocolo de volume remoto NetApp
iscsi	3260/TCP	Porta de destino iSCSI
Lockd	4045/TCP 4045/UDP	Daemon de bloqueio NFS
NFS	4046/TCP	Protocolo de montagem NFS
acp-proto	4046/UDP	Protocolo de contabilidade
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Segurança do protocolo da Internet
acp	5125/UDP 5133/UDP 5144/TCP	Porta de controle alternativa para disco
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS: Protocolo binário de escuta
TELNET	8023/TCP	Telnet com escopo de nó
HTTPS	8443/TCP	Ferramenta GUI 7MTT através do xref:./ontap-security-hardening/HTTPS
RSH	8514/TCP	RSH do nó-escopo

Serviço	Porta/protocolo	Descrição
`KMIP`	9877/TCP	Porta de cliente KMIP (somente host local interno)
`ndmp`	10000/TCP	NDMP
`cifs` testemunha do porto	40001/TCP	Porta de testemunhas CIFS
`TLS`	50000/TCP	Segurança da camada de transporte
`Iscsi`	65200/TCP	Porta iSCSI
`SSH`	65502/TCP	Shell seguro
`vsun`	65503/TCP	vsun

Portas internas do NetApp

Porta/protocolo	Descrição
900	RPC de cluster NetApp
902	RPC de cluster NetApp
904	RPC de cluster NetApp
905	RPC de cluster NetApp
910	RPC de cluster NetApp
911	RPC de cluster NetApp
913	RPC de cluster NetApp
914	RPC de cluster NetApp
915	RPC de cluster NetApp
918	RPC de cluster NetApp
920	RPC de cluster NetApp
921	RPC de cluster NetApp
924	RPC de cluster NetApp
925	RPC de cluster NetApp
927	RPC de cluster NetApp
928	RPC de cluster NetApp
929	RPC de cluster NetApp
931	RPC de cluster NetApp
932	RPC de cluster NetApp
933	RPC de cluster NetApp
934	RPC de cluster NetApp
935	RPC de cluster NetApp
936	RPC de cluster NetApp

Porta/protocolo	Descrição
937	RPC de cluster NetApp
939	RPC de cluster NetApp
940	RPC de cluster NetApp
951	RPC de cluster NetApp
954	RPC de cluster NetApp
955	RPC de cluster NetApp
956	RPC de cluster NetApp
958	RPC de cluster NetApp
961	RPC de cluster NetApp
963	RPC de cluster NetApp
964	RPC de cluster NetApp
966	RPC de cluster NetApp
967	RPC de cluster NetApp
7810	RPC de cluster NetApp
7811	RPC de cluster NetApp
7812	RPC de cluster NetApp
7813	RPC de cluster NetApp
7814	RPC de cluster NetApp
7815	RPC de cluster NetApp
7816	RPC de cluster NetApp
7817	RPC de cluster NetApp
7818	RPC de cluster NetApp
7819	RPC de cluster NetApp
7820	RPC de cluster NetApp
7821	RPC de cluster NetApp
7822	RPC de cluster NetApp
7823	RPC de cluster NetApp
7824	RPC de cluster NetApp

Auditar eventos nas em SVMs

Auditoria de SMB e NFS e rastreamento de segurança

Você pode usar os recursos de auditoria de acesso a arquivos disponíveis para os protocolos SMB e NFS com o ONTAP, como auditoria nativa e gerenciamento de

políticas de arquivos usando FPolicy.

Você deve projetar e implementar a auditoria de eventos de acesso a arquivos SMB e NFS nas seguintes circunstâncias:

- O acesso básico a arquivos de protocolo SMB e NFS foi configurado.
- Você deseja criar e manter uma configuração de auditoria usando um dos seguintes métodos:
  - Funcionalidade ONTAP nativa
  - Servidores FPolicy externos

Auditar eventos nas em SVMs

A auditoria de eventos nas é uma medida de segurança que permite controlar e Registrar determinados eventos SMB e NFS em máquinas virtuais de storage (SVMs). Isso ajuda você a rastrear possíveis problemas de segurança e fornece evidências de quaisquer violações de segurança. Você também pode organizar e auditar políticas de acesso central do ative Directory para ver qual seria o resultado da implementação delas.

Eventos SMB

Você pode auditar os seguintes eventos:

- Eventos de acesso a arquivos SMB e pastas

  Você pode auditar eventos de acesso a arquivos SMB e pastas em objetos armazenados em volumes FlexVol pertencentes aos SVMs habilitados para auditoria.

- Eventos de logon e logoff SMB

  Você pode auditar eventos de logon e logoff SMB para servidores SMB em SVMs.

- Eventos de preparação da política de acesso central

  Você pode auditar o acesso efetivo de objetos em servidores SMB usando permissões aplicadas por meio de políticas de acesso centrais propostas. A auditoria por meio do preparo de políticas de acesso central permite que você veja quais são os efeitos das políticas de acesso centrais antes que elas sejam implantadas.

  A auditoria do preparo de políticas de acesso central é configurada usando GPOs do active Directory. No entanto, a configuração de auditoria SVM deve ser configurada para auditar eventos de preparação de políticas de acesso central.

  Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, os eventos de estadiamento da política de acesso central são gerados somente se o Controle de Acesso Dinâmico estiver ativado. O Dynamic Access Control é ativado através de uma opção de servidor SMB. Ele não está habilitado por padrão.

Eventos NFS

Você pode auditar eventos de arquivo e diretório utilizando NFSv4 ACL em objetos armazenados em SVMs.

Como funciona a auditoria

Conceitos básicos de auditoria

Para entender a auditoria no ONTAP, você deve estar ciente de alguns conceitos básicos de auditoria.

- **Staging arquivos**

  Os arquivos binários intermediários em nós individuais onde os Registros de auditoria são armazenados antes da consolidação e conversão. Os arquivos de estadiamento estão contidos nos volumes de estadiamento.

- * Volume de estadiamento*

  Um volume dedicado criado pelo ONTAP para armazenar arquivos de teste. Há um volume de estadiamento por agregado. Os volumes de preparo são compartilhados por todas as máquinas virtuais de armazenamento (SVMs) habilitadas para auditoria para armazenar Registros de auditoria do acesso a dados para volumes de dados nesse agregado específico. Os Registros de auditoria de cada SVM são armazenados em um diretório separado dentro do volume de teste.

  Os administradores de cluster podem exibir informações sobre volumes de teste, mas a maioria das outras operações de volume não são permitidas. Somente o ONTAP pode criar volumes de estadiamento. O ONTAP atribui automaticamente um nome aos volumes de teste. Todos os nomes de volume de estadiamento começam com `MDV_aud_` seguido pelo UUID do agregado que contém esse volume de estadiamento (por exemplo: `MDV_aud_1d0131843d4811e296fc123478563412` .)

- **Volumes do sistema**

  Um FlexVol volume que contém metadados especiais, como metadados para logs de auditoria de serviços de arquivo. O SVM admin é proprietário de volumes de sistema, que podem ser vistos no cluster. Os volumes de estadiamento são um tipo de volume do sistema.

- **Tarefa de consolidação**

  Uma tarefa que é criada quando a auditoria é ativada. Essa tarefa de longa execução em cada SVM leva os Registros de auditoria de arquivos de teste nos nós membros do SVM. Essa tarefa mescla os Registros de auditoria em ordem cronológica ordenada e os converte em um formato de log de eventos legível pelo usuário especificado na configuração de auditoria — o formato de arquivo EVTX ou XML. Os logs de eventos convertidos são armazenados no diretório de log de eventos de auditoria especificado na configuração de auditoria SVM.

Como funciona o processo de auditoria do ONTAP

O processo de auditoria do ONTAP é diferente do processo de auditoria da Microsoft. Antes de configurar a auditoria, você deve entender como o processo de auditoria do ONTAP funciona.

Os Registros de auditoria são inicialmente armazenados em arquivos de estadiamento binários em nós individuais. Se a auditoria estiver habilitada em uma SVM, cada nó de membro manterá os arquivos de teste para essa SVM. Periodicamente, eles são consolidados e convertidos em logs de eventos legíveis pelo usuário, que são armazenados no diretório de log de eventos de auditoria do SVM.

Processo quando a auditoria é ativada em uma SVM

A auditoria só pode ser ativada em SVMs. Quando o administrador de storage habilita a auditoria na SVM, o subsistema de auditoria verifica se há volumes de teste presentes. Deve existir um volume de preparo para cada agregado que contenha volumes de dados de propriedade da SVM. O subsistema de auditoria cria todos os volumes de teste necessários se eles não existirem.

O subsistema de auditoria também conclui outras tarefas de pré-requisito antes que a auditoria seja ativada:

- O subsistema de auditoria verifica se o caminho do diretório de log está disponível e não contém links simbólicos.

  O diretório de log já deve existir como um caminho dentro do namespace do SVM. Recomenda-se criar um novo volume ou qtree para manter os arquivos de log de auditoria. O subsistema de auditoria não atribui um local de arquivo de log padrão. Se o caminho do diretório de log especificado na configuração de auditoria não for um caminho válido, a criação da configuração de auditoria falhará com o `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` erro.

  A criação de configuração falha se o diretório existir, mas contiver links simbólicos.

- A auditoria agenda a tarefa de consolidação.

  Depois que esta tarefa é agendada, a auditoria é ativada. A configuração de auditoria SVM e os arquivos de log persistem em uma reinicialização ou se os servidores NFS ou SMB forem interrompidos ou reiniciados.

Consolidação do log de eventos

A consolidação de log é uma tarefa agendada que é executada de rotina até que a auditoria seja desativada. Quando a auditoria é desativada, a tarefa de consolidação verifica se todos os logs restantes estão consolidados.

Auditoria garantida

Por padrão, a auditoria é garantida. O ONTAP garante que todos os eventos de acesso a arquivos auditáveis (conforme especificado pelas ACLs de diretiva de auditoria configuradas) sejam registrados, mesmo que um nó não esteja disponível. Uma operação de arquivo solicitada não pode ser concluída até que o Registro de auditoria dessa operação seja salvo no volume de espera no armazenamento persistente. Se os Registros de auditoria não puderem ser comprometidos com o disco nos arquivos de teste, seja por causa de espaço insuficiente ou por causa de outros problemas, as operações do cliente serão negadas.

> Um administrador ou usuário de conta com acesso em nível de privilégio pode ignorar a operação de log de auditoria de arquivos usando o SDK de gerenciamento do NetApp ou APIs REST. Você pode determinar se alguma ação de arquivo foi realizada usando o SDK de gerenciamento do NetApp ou APIs REST, revisando os logs do histórico de comandos armazenados no `audit.log` arquivo.
>
> Para obter mais informações sobre logs de auditoria do histórico de comandos, consulte a seção "Gerenciando logs de auditoria para atividades de gerenciamento" no "Administração do sistema".

Processo de consolidação quando um nó não está disponível

Se um nó que contenha volumes pertencentes a uma SVM com auditoria habilitada não estiver disponível, o comportamento da tarefa de consolidação de auditoria depende se o parceiro de failover de storage (SFO) do nó (ou o parceiro de HA no caso de um cluster de dois nós) está disponível:

- Se o volume de estadiamento estiver disponível por meio do parceiro SFO, os volumes de estadiamento relatados pela última vez pelo nó serão verificados e a consolidação continuará normalmente.
- Se o parceiro SFO não estiver disponível, a tarefa criará um arquivo de log parcial.

  Quando um nó não é alcançável, a tarefa de consolidação consolida os Registros de auditoria dos outros nós disponíveis desse SVM. Para identificar que não está concluída, a tarefa adiciona o sufixo `.partial` ao nome do arquivo consolidado.

- Depois que o nó indisponível estiver disponível, os Registros de auditoria nesse nó serão consolidados com os Registros de auditoria dos outros nós naquele momento.
- Todos os Registros de auditoria são preservados.

Rotação do registo de eventos

Os arquivos de log de eventos de auditoria são girados quando atingem um tamanho de log de limite configurado ou em uma programação configurada. Quando um arquivo de log de eventos é girado, a tarefa de consolidação agendada primeiro renomeia o arquivo convertido ativo para um arquivo de arquivo com carimbo de tempo e, em seguida, cria um novo arquivo de log de eventos convertido ativo.

Processo quando a auditoria é desativada no SVM

Quando a auditoria é desativada na SVM, a tarefa de consolidação é acionada uma última vez. Todos os Registros de auditoria registrados pendentes são registrados em um formato legível pelo usuário. Os logs de eventos existentes armazenados no diretório de log de eventos não são excluídos quando a auditoria é desativada no SVM e estão disponíveis para visualização.

Depois que todos os arquivos de teste existentes para esse SVM forem consolidados, a tarefa de consolidação será removida da programação. A desativação da configuração de auditoria do SVM não remove a configuração de auditoria. Um administrador de storage pode reativar a auditoria a qualquer momento.

A tarefa de consolidação de auditoria, que é criada quando a auditoria é ativada, monitora a tarefa de consolidação e a cria novamente se a tarefa de consolidação sair devido a um erro. Os usuários não podem excluir o trabalho de consolidação de auditoria.

Requisitos e considerações de auditoria

Antes de configurar e habilitar a auditoria na máquina virtual de storage (SVM), é necessário estar ciente de certos requisitos e considerações.

- O número máximo de SVMs habilitadas para auditoria suportado depende da sua versão do ONTAP:

Versão de ONTAP	Máximo
9,8 e anteriores	50
9.9.1 e mais tarde	400

- A auditoria não está vinculada ao licenciamento SMB ou NFS.

  Você pode configurar e ativar a auditoria mesmo que as licenças SMB e NFS não estejam instaladas no cluster.

- A auditoria NFS dá suporte a ACEs de segurança (tipo U).
- Para auditoria NFS, não há mapeamento entre bits de modo e ACEs de auditoria.

  Ao converter ACLs em bits de modo, os ACEs de auditoria são ignorados. Ao converter bits de modo para ACLs, os ACEs de auditoria não são gerados.

- O diretório especificado na configuração de auditoria deve existir.

  Se não existir, o comando para criar a configuração de auditoria falha.

- O diretório especificado na configuração de auditoria deve atender aos seguintes requisitos:
  - O diretório não deve conter links simbólicos.

    Se o diretório especificado na configuração de auditoria contiver links simbólicos, o comando para criar a configuração de auditoria falhará.

  - Você deve especificar o diretório usando um caminho absoluto.

    Você não deve especificar um caminho relativo, por exemplo `/vs1/../`, .

- A auditoria depende de ter espaço disponível nos volumes de teste.

  Você deve estar ciente e ter um plano para garantir que haja espaço suficiente para os volumes de teste em agregados que contenham volumes auditados.

- A auditoria depende de ter espaço disponível no volume que contém o diretório onde os logs de eventos convertidos são armazenados.

  Você deve estar ciente e ter um plano para garantir que há espaço suficiente nos volumes usados para armazenar logs de eventos. Você pode especificar o número de logs de eventos a serem mantidos no diretório de auditoria usando o `-rotate-limit` parâmetro ao criar uma configuração de auditoria, o que pode ajudar a garantir que haja espaço disponível suficiente para os logs de eventos no volume.

- Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, o Controle de Acesso Dinâmico deve estar habilitado para gerar eventos de estadiamento da política de acesso central.

  O controlo de Acesso Dinâmico não está ativado por predefinição.

Agregue considerações de espaço ao ativar a auditoria

Quando uma configuração de auditoria é criada e a auditoria é ativada em pelo menos uma máquina virtual de storage (SVM) no cluster, o subsistema de auditoria cria volumes de teste em todos os agregados existentes e em todos os novos agregados criados. Você precisa estar ciente de certas considerações de espaço agregado ao habilitar a auditoria no cluster.

A criação de volume de estadiamento pode falhar devido à não disponibilidade de espaço em um agregado. Isso pode acontecer se você criar uma configuração de auditoria e os agregados existentes não tiverem espaço suficiente para conter o volume de preparo.

Você deve garantir que haja espaço suficiente nos agregados existentes para os volumes de teste antes de habilitar a auditoria em um SVM.

Limitações para o tamanho dos Registros de auditoria em arquivos de teste

O tamanho de um Registro de auditoria em um arquivo de teste não pode ser maior que 32 KB.

Quando grandes Registros de auditoria podem ocorrer

Grandes Registros de auditoria podem ocorrer durante a auditoria de gerenciamento em um dos seguintes cenários:

- Adicionar ou excluir usuários de ou para grupos com um grande número de usuários.
- Adicionar ou excluir uma lista de controle de acesso de compartilhamento de arquivos (ACL) em um compartilhamento de arquivos com um grande número de usuários de compartilhamento de arquivos.
- Outros cenários.

Desative a auditoria de gerenciamento para evitar esse problema. Para fazer isso, modifique a configuração de auditoria e remova o seguinte da lista de tipos de eventos de auditoria:

- compartilhamento de arquivos
- conta de utilizador
- grupo de segurança
- autorização-política-alteração

  Após a remoção, eles não serão auditados pelo subsistema de auditoria de serviços de arquivo.

Os efeitos dos registos de auditoria demasiado grandes

- Se o tamanho de um Registro de auditoria for muito grande (mais de 32 KB), o Registro de auditoria não será criado e o subsistema de auditoria gerará uma mensagem do sistema de gerenciamento de eventos (EMS) semelhante à seguinte:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  Se a auditoria for garantida, a operação do arquivo falhará porque seu Registro de auditoria não pode ser criado.

- Se o tamanho do registo de auditoria for superior a 9.999 bytes, é apresentada a mesma mensagem EMS acima. Um Registro de auditoria parcial é criado com o valor de chave maior ausente.
- Se o Registro de auditoria exceder 2.000 carateres, a seguinte mensagem de erro será exibida em vez do valor real:

  ```
  The value of this field was too long to display.
  ```

Quais são os formatos de log de eventos de auditoria suportados

Os formatos de arquivo suportados para os logs de eventos de auditoria convertidos são `EVTX` e `XML` formatos de arquivo.

Você pode especificar o tipo de formato de arquivo ao criar a configuração de auditoria. Por padrão, o ONTAP converte os logs binários para o `EVTX` formato de arquivo.

Ver registos de eventos de auditoria

Você pode usar logs de eventos de auditoria para determinar se você tem segurança de arquivo adequada e se houve tentativas inadequadas de acesso a arquivos e pastas. Pode visualizar e processar registos de eventos de auditoria guardados nos `EVTX` formatos de ficheiro ou `XML`.

- `EVTX` formato do ficheiro

  Você pode abrir os logs de eventos de auditoria convertidos `EVTX` como arquivos salvos usando o Visualizador de Eventos da Microsoft.

  Há duas opções que você pode usar ao visualizar logs de eventos usando o Visualizador de eventos:

  - Vista geral

    As informações comuns a todos os eventos são exibidas para o Registro de eventos. Nesta versão do ONTAP, os dados específicos do evento para o Registro de eventos não são exibidos. Você pode usar a exibição detalhada para exibir dados específicos do evento.

  - Vista detalhada

    Uma vista amigável e uma vista XML estão disponíveis. A visualização amigável e a visualização XML exibem as informações comuns a todos os eventos e os dados específicos do evento para o Registro de eventos.

- `XML` formato do ficheiro

  Você pode exibir e processar `XML` logs de eventos de auditoria em aplicativos de terceiros que suportam o `XML` formato de arquivo. As ferramentas de visualização XML podem ser usadas para visualizar os logs de auditoria, desde que você tenha o esquema XML e informações sobre definições para os campos XML. Para obter mais informações sobre o esquema XML e definições, consulte "Referência de Esquema de Auditoria ONTAP" .

Como os logs de auditoria ativos são visualizados usando o Visualizador de Eventos

Se o processo de consolidação de auditoria estiver em execução no cluster, o processo de consolidação anexará novos Registros ao arquivo de log de auditoria ativo para máquinas virtuais de armazenamento (SVMs) habilitadas para auditoria. Este log de auditoria ativo pode ser acessado e aberto por meio de um compartilhamento SMB no Visualizador de Eventos da Microsoft.

Além de exibir Registros de auditoria existentes, o Visualizador de Eventos tem uma opção de atualização que permite atualizar o conteúdo na janela do console. Se os logs recém-anexados são visíveis no Visualizador de Eventos depende se os oplocks estão ativados no compartilhamento usado para acessar o log de auditoria

ativo.

Definição de Oplocks na partilha	Comportamento
Ativado	O Visualizador de Eventos abre o log que contém eventos gravados até esse ponto no tempo. A operação de atualização não atualiza o log com novos eventos anexados pelo processo de consolidação.
Desativado	O Visualizador de Eventos abre o log que contém eventos gravados até esse ponto no tempo. A operação de atualização atualiza o log com novos eventos anexados pelo processo de consolidação.

Esta informação é aplicável apenas para `EVTX` registos de eventos. `XML` Os logs de eventos podem ser visualizados através de SMB em um navegador ou através de NFS usando qualquer editor ou visualizador XML.

Eventos SMB que podem ser auditados

Visão geral de eventos SMB que podem ser auditados

O ONTAP pode auditar determinados eventos SMB, incluindo determinados eventos de acesso a arquivos e pastas, determinados eventos de logon e logoff e eventos de preparação de políticas de acesso central. Saber quais eventos de acesso podem ser auditados é útil ao interpretar os resultados dos logs de eventos.

Os seguintes eventos SMB adicionais podem ser auditados no ONTAP 9.2 e posteriores:

ID DO EVENTO (EVT/EVTX)	Evento	Descrição	Categoria
4670	As permissões do objeto foram alteradas	ACESSO A OBJETO: Permissões alteradas.	Acesso a ficheiros
4907	As definições de auditoria de objetos foram alteradas	ACESSO A OBJETO: Definições de auditoria alteradas.	Acesso a ficheiros
4913	A Política de Acesso Central Objeto foi alterada	ACESSO A OBJETO: CAP ALTERADO.	Acesso a ficheiros

Os seguintes eventos SMB podem ser auditados no ONTAP 9.0 e posteriores:

ID DO EVENTO (EVT/EVTX)	Evento	Descrição	Categoria
540/4624	Uma conta foi iniciada com êxito	Logon/LOGOFF: Logon em rede (SMB).	Início de sessão e fim de sessão

529/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Nome de usuário desconhecido ou senha ruim.	Início de sessão e fim de sessão
530/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Restrição de tempo de logon da conta.	Início de sessão e fim de sessão
531/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Conta atualmente desativada.	Início de sessão e fim de sessão
532/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: A conta de usuário expirou.	Início de sessão e fim de sessão
533/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O usuário não pode fazer logon neste computador.	Início de sessão e fim de sessão
534/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O usuário não recebeu o tipo de logon aqui.	Início de sessão e fim de sessão
535/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: A senha do usuário expirou.	Início de sessão e fim de sessão
537/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O logon falhou por motivos diferentes dos acima.	Início de sessão e fim de sessão
539/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Conta bloqueada.	Início de sessão e fim de sessão
538/4634	Uma conta foi encerrada	Logon/LOGOFF: LOGOFF de usuário local ou de rede.	Início de sessão e fim de sessão
560/4656	Abrir Objeto/criar Objeto	ACESSO A OBJETO: Objeto (arquivo ou diretório) aberto.	Acesso a ficheiros
563/4659	Abra Objeto com a intenção de Excluir	ACESSO A OBJETO: Um identificador para um objeto (arquivo ou diretório) foi solicitado com o intent to Delete.	Acesso a ficheiros
564/4660	Eliminar Objeto	ACESSO A OBJETO: Excluir Objeto (arquivo ou diretório). O ONTAP gera esse evento quando um cliente Windows tenta excluir o objeto (arquivo ou diretório).	Acesso a ficheiros

567/4663	Ler Objeto/escrever Objeto/obter atributos Objeto/Definir atributos Objeto	ACESSO A OBJETO: Tentativa de acesso a objeto (ler, escrever, obter atributo, definir atributo). **Observação:** para este evento, o ONTAP audita apenas a primeira operação de leitura e gravação SMB (sucesso ou falha) em um objeto. Isso impede que o ONTAP crie entradas de log excessivas quando um único cliente abre um objeto e executa muitas operações de leitura ou gravação sucessivas no mesmo objeto.	Acesso a ficheiros
NA/4664	Link físico	ACESSO A OBJETOS: Foi feita uma tentativa de criar um link físico.	Acesso a ficheiros
NA/4818	A política de acesso central proposta não concede as mesmas permissões de acesso que a política de acesso central atual	ACESSO A OBJETOS: Central Access Policy Staging.	Acesso a ficheiros
ID do evento Data ONTAP NA/na 9999	Mudar o nome do objeto	ACESSO A OBJETO: Objeto renomeado. Este é um evento da ONTAP. Atualmente, não é suportado pelo Windows como um único evento.	Acesso a ficheiros
ID do evento Data ONTAP NA/na 9998	Desvincular Objeto	ACESSO A OBJETO: Objeto não vinculado. Este é um evento da ONTAP. Atualmente, não é suportado pelo Windows como um único evento.	Acesso a ficheiros

Informações adicionais sobre o evento 4656

A `HandleID` tag no evento de auditoria `XML` contém o identificador do objeto (arquivo ou diretório) acessado. A `HandleID` tag para o evento EVTX 4656 contém informações diferentes, dependendo se o evento aberto é para criar um novo objeto ou para abrir um objeto existente:

- Se o evento aberto for uma solicitação aberta para criar um novo objeto (arquivo ou diretório), a `HandleID` tag no evento XML de auditoria mostrará um vazio `HandleID` (por exemplo: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  O `HandleID` está vazio porque a SOLICITAÇÃO ABERTA (para criar um novo objeto) é auditada antes da criação real do objeto acontecer e antes de existir um identificador. Eventos auditados subsequentes para o mesmo objeto têm o identificador de objeto certo na `HandleID` tag.

- Se o evento aberto for uma solicitação aberta para abrir um objeto existente, o evento de auditoria terá o identificador atribuído desse objeto na `HandleID` tag (por exemplo: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determine qual é o caminho completo para o objeto auditado

O caminho do objeto impresso na `<ObjectName>` tag para um Registro de auditoria contém o nome do volume (entre parênteses) e o caminho relativo da raiz do volume que contém. Se você quiser determinar o caminho completo do objeto auditado, incluindo o caminho de junção, há certas etapas que você deve seguir.

Passos

1. Determine qual é o nome do volume e o caminho relativo para o objeto auditado olhando para a `<ObjectName>` tag no evento de auditoria.

   Neste exemplo, o nome do volume é "ATA1" e o caminho relativo para o arquivo é `/dir1/file.txt`:

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. Usando o nome do volume determinado na etapa anterior, determine qual é o caminho de junção para o volume que contém o objeto auditado:

   Neste exemplo, o nome do volume é "ATA1" e o caminho de junção para o volume que contém o objeto auditado é `/data/data1`:

   ```
   volume show -junction -volume data1
   ```

   ```
                                Junction                       Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. Determine o caminho completo para o objeto auditado anexando o caminho relativo encontrado na `<ObjectName>` tag para o caminho de junção para o volume.

   Neste exemplo, o caminho de junção para o volume:

   ```
   /data/data1/dir1/file.text
   ```

Considerações ao auditar links simbólicos e links duros

Há certas considerações que você deve ter em mente ao auditar links simbólicos e links duros.

Um Registro de auditoria contém informações sobre o objeto que está sendo auditado, incluindo o caminho para o objeto auditado, que é identificado na `ObjectName` tag. Você deve estar ciente de como caminhos para links simbólicos e links rígidos são gravados na `ObjectName` tag.

Links simbólicos

Um link simbólico é um arquivo com um inode separado que contém um ponteiro para a localização de um objeto de destino, conhecido como alvo. Ao acessar um objeto por meio de um link simbólico, o ONTAP interpreta automaticamente o link simbólico e segue o caminho agnóstico do protocolo canônico real para o objeto de destino no volume.

Na saída de exemplo a seguir, há dois links simbólicos, ambos apontando para um arquivo `target.txt` chamado . Um dos links simbólicos é um link simbólico relativo e um é um link simbólico absoluto. Se qualquer um dos links simbólicos for auditado, a `ObjectName` tag no evento de auditoria conterá o caminho para o arquivo `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Links físicos

Um link físico é uma entrada de diretório que associa um nome a um arquivo existente em um sistema de arquivos. O link físico aponta para a localização do inode do arquivo original. Semelhante a como o ONTAP interpreta links simbólicos, o ONTAP interpreta o link físico e segue o caminho canônico real para o objeto alvo no volume. Quando o acesso a um objeto de link físico é auditado, o evento de auditoria Registra esse caminho canônico absoluto na `ObjectName` tag em vez do caminho do link físico.

Considerações ao auditar fluxos de dados NTFS alternativos

Há certas considerações que você deve ter em mente ao auditar arquivos com fluxos de dados alternativos NTFS.

A localização de um objeto que está sendo auditado é registrada em um Registro de evento usando duas tags, a `ObjectName` tag (o caminho) e a `HandleID` tag (o identificador). Para identificar corretamente quais solicitações de fluxo estão sendo registradas, você deve estar ciente de quais Registros do ONTAP nesses campos para fluxos de dados alternativos do NTFS:

- ID EVTX: 4656 eventos (abrir e criar eventos de auditoria)
  - O caminho do fluxo de dados alternativo é gravado na `ObjectName` tag.
  - O identificador do fluxo de dados alternativo é gravado na `HandleID` tag.
- ID EVTX: 4663 eventos (todos os outros eventos de auditoria, como leitura, escrita, getattr, e assim por diante)
  - O caminho do arquivo base, não o fluxo de dados alternativo, é gravado na `ObjectName` tag.
  - O identificador do fluxo de dados alternativo é gravado na `HandleID` tag.

Exemplo

O exemplo a seguir ilustra como identificar o ID EVTX: 4663 eventos para fluxos de dados alternativos usando a `HandleID` tag. Mesmo que a `ObjectName` tag (caminho) registrada no evento de auditoria de leitura seja

para o caminho do arquivo base, a `HandleID` tag pode ser usada para identificar o evento como um Registro de auditoria para o fluxo de dados alternativo.

Os nomes dos arquivos de stream assumem o formulário `base_file_name:stream_name`. Neste exemplo, o `dir1` diretório contém um arquivo base com um fluxo de dados alternativo com os seguintes caminhos:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

A saída no exemplo de evento a seguir é truncada como indicado; a saída não exibe todas as tags de saída disponíveis para os eventos.

Para um EVTX ID 4656 (evento de auditoria aberto), a saída do Registro de auditoria para o fluxo de dados alternativo Registra o nome do fluxo de dados alternativo na `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

Para um EVTX ID 4663 (evento de auditoria de leitura), a saída do Registro de auditoria para o mesmo fluxo de dados alternativo Registra o nome do arquivo base na `ObjectName` tag; no entanto, o identificador na `HandleID` tag é o identificador do fluxo de dados alternativo e pode ser usado para correlacionar esse evento com o fluxo de dados alternativo:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Eventos de acesso a arquivos e diretórios NFS que podem ser auditados

O ONTAP pode auditar determinados eventos de acesso a arquivos NFS e diretórios. Saber quais eventos de acesso podem ser auditados é útil ao interpretar os resultados dos logs de eventos de auditoria convertidos.

Você pode auditar os seguintes eventos de acesso a arquivos NFS e diretórios:

- LEIA
- ABRIR
- FECHAR
- READDIR
- ESCREVA
- SETATTR
- CRIAR
- LINK
- OPENATTR
- RETIRE
- GETATTR
- VERIFIQUE
- NVERIFY
- MUDAR O NOME

Para auditar de forma confiável os eventos DE RENOMEAÇÃO do NFS, você deve definir ACEs de auditoria em diretórios em vez de arquivos porque as permissões de arquivo não são verificadas para uma operação DE RENOMEAÇÃO se as permissões de diretório forem suficientes.

Planejar a configuração de auditoria

Antes de configurar a auditoria em máquinas virtuais de armazenamento (SVMs), você deve entender quais opções de configuração estão disponíveis e Planejar os valores que deseja definir para cada opção. Essas informações podem ajudá-lo a configurar a configuração de auditoria que atende às necessidades da sua empresa.

Existem certos parâmetros de configuração que são comuns a todas as configurações de auditoria.

Além disso, existem certos parâmetros que você pode usar para especificar quais métodos são usados ao girar os logs de auditoria consolidados e convertidos. Você pode especificar um dos três métodos a seguir ao configurar a auditoria:

- Rode registos com base no tamanho do registo

  Este é o método padrão usado para girar logs.

- Gire os logs com base em um agendamento
- Rodar registos com base no tamanho e na programação do registo (qualquer que seja o evento que ocorrer primeiro)

Pelo menos um dos métodos de rotação de log deve ser sempre definido.

Parâmetros comuns a todas as configurações de auditoria

Há dois parâmetros necessários que você deve especificar ao criar a configuração de auditoria. Há também três parâmetros opcionais que você pode especificar:

Tipo de informação	Opção	Obrigatório	Incluir	Seus valores
Nome da SVM Nome do SVM no qual você pode criar a configuração de auditoria. O SVM já deve existir.	`-vserver vserver_name`	Sim	Sim	

Log Destination path Especifica o diretório onde os logs de auditoria convertidos são armazenados, normalmente um volume ou qtree dedicado. O caminho já deve existir no namespace SVM. O caminho pode ter até 864 carateres de comprimento e deve ter permissões de leitura e gravação. Se o caminho não for válido, o comando de configuração de auditoria falhará. Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino do log não poderá estar no volume raiz. Isso ocorre porque o conteúdo do volume raiz não é replicado para o destino de recuperação de desastres. Não é possível usar um volume FlexCache como destino de log (ONTAP 9.7 e posterior).	`-destination text`	Sim	Sim	

Categorias de eventos a auditar Especifica as categorias de eventos a auditar. As seguintes categorias de eventos podem ser auditadas: • Eventos de acesso a arquivos (SMB e NFSv4) • Eventos de logon e logoff SMB • Eventos de preparação da política de acesso central Os eventos de preparação da política de acesso central estão disponíveis a partir dos domínios do ative Directory do Windows 2012. • Eliminação assíncrona • Eventos de categoria de compartilhamento de arquivos • Auditoria de eventos de mudança de política • Eventos de gerenciamento de contas de usuário local • Eventos de gerenciamento de grupo de segurança • Eventos de alteração da política de autorização O padrão é auditar o acesso a arquivos e eventos de logon e logoff SMB. **Observação:** antes de poder especificar `cap-staging` como categoria de evento, um servidor SMB deve existir na SVM. Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, os eventos de estadiamento da política de acesso central são gerados somente se o Controle de Acesso Dinâmico estiver ativado. O Dynamic Access Control é ativado através de uma opção de servidor SMB. Ele não está habilitado por padrão.	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`

audit-policy-change	user-account	security-group	authorization-policy-change	`async-delete`Selecione
Não			*Formato de saída do ficheiro de registo* Determina o formato de saída dos logs de auditoria. O formato de saída pode ser um formato de log específico do ONTAP XML ou do Microsoft Windows EVTX. Por padrão, o formato de saída é EVTX.	-format {xml

`evtx`Selecione	Não			*Limite de rotação de arquivos de log* Determina quantos arquivos de log de auditoria devem ser mantidos antes de girar o arquivo de log mais antigo. Por exemplo, se você inserir um valor de `5`, os últimos cinco arquivos de log serão retidos. Um valor de `0` indica que todos os arquivos de log são mantidos. O valor padrão é 0.

Parâmetros usados para determinar quando girar logs de eventos de auditoria

Rotate logs com base no tamanho do log

O padrão é girar os logs de auditoria com base no tamanho.

- O tamanho padrão do log é de 100 MB
- Se você quiser usar o método de rotação de log padrão e o tamanho padrão do log, não será necessário configurar nenhum parâmetro específico para a rotação de log.
- Se você quiser girar os logs de auditoria somente com base em um tamanho de log, use o seguinte comando para desdefinir o `-rotate-schedule-minute` parâmetro: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Se você não quiser usar o tamanho padrão do log, você pode configurar o `-rotate-size` parâmetro para especificar um tamanho de log personalizado:

Tipo de informação	Opção	Obrigatório	Incluir	Seus valores
Limite de tamanho do ficheiro de registo Determina o limite de tamanho do arquivo de log de auditoria.	`-rotate-size` {`integer`[KB	MB	GB	TB

Rotate logs com base em uma programação

Se você optar por girar os logs de auditoria com base em um agendamento, poderá agendar a rotação de logs usando os parâmetros de rotação baseados em tempo em qualquer combinação.

- Se utilizar rotação baseada no tempo, o `-rotate-schedule-minute` parâmetro é obrigatório.
- Todos os outros parâmetros de rotação baseados no tempo são opcionais.
- O programa de rotação é calculado utilizando todos os valores relacionados com o tempo.

  Por exemplo, se você especificar apenas o `-rotate-schedule-minute` parâmetro, os arquivos de log de auditoria serão girados com base nos minutos especificados em todos os dias da semana, durante todas as horas em todos os meses do ano.

- Se você especificar apenas um ou dois parâmetros de rotação baseados no tempo (por exemplo, `-rotate-schedule-month` e `-rotate-schedule-minutes`), os arquivos de log serão girados com base nos valores de minuto especificados em todos os dias da semana, durante todas as horas, mas somente durante os meses especificados.

  Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro, março e agosto em todas as segundas, quartas e sábados às 10:30 da manhã

- Se você especificar valores para ambos `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, eles serão considerados independentemente.

  Por exemplo, se você especificar `-rotate-schedule-dayofweek` como sexta-feira e `-rotate -schedule-day` como 13, os logs de auditoria serão girados em todas as sextas-feiras e no dia 13th do mês especificado, não apenas em todas as sextas-feiras, dia 13th.

- Se você quiser girar os logs de auditoria somente com base em uma programação, use o seguinte comando para desdefinir o `-rotate-size` parâmetro: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Você pode usar a seguinte lista de parâmetros de auditoria disponíveis para determinar quais valores usar para configurar uma programação para rotações de log de eventos de auditoria:

Tipo de informação	Opção	Obrigatório	Incluir	Seus valores
Calendário de rotação de Registro: Mês Determina a programação mensal para os logs de auditoria rotativos. Os valores válidos `January` são através de `December`, e `all`. Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro, março e agosto.	`-rotate-schedule-month chron_month`	Não		
Calendário de rotação de Registro: Dia da semana Determina o cronograma diário (dia da semana) para logs de auditoria rotativos. Os valores válidos `Sunday` são através de `Saturday`, e `all`. Por exemplo, você pode especificar que o log de auditoria deve ser girado às terças e sextas-feiras, ou durante todos os dias de uma semana.	`-rotate-schedule -dayofweek chron_dayofweek`	Não		
Calendário de rotação de Registro: Dia Determina o dia do calendário do mês para a rotação do log de auditoria. Os valores válidos variam de `1` até `31`. Por exemplo, você pode especificar que o log de auditoria deve ser girado nos 10th e 20th dias de um mês ou em todos os dias de um mês.	`-rotate-schedule-day chron_dayofmonth`	Não		
Calendário de rotação de Registro: Hora Determina a programação horária para girar o log de auditoria. Os valores válidos variam de `0` (meia-noite) a `23` (11:00 p.m.). `all`Especificar gira os logs de auditoria a cada hora. Por exemplo, você pode especificar que o log de auditoria deve ser girado às 6 (6 a.m.) e 18 (6 p.m.).	`-rotate-schedule-hour chron_hour`	Não		

Calendário de rotação de Registro: Minuto Determina o cronograma de minutos para girar o log de auditoria. Os valores válidos variam de `0` a `59`. Por exemplo, você pode especificar que o log de auditoria deve ser girado aos 30th minutos.	`-rotate-schedule-minute chron_minute`	Sim, se configurar a rotação de log baseada em programação; caso contrário, não		

Rotate logs com base no tamanho e horário do log

Você pode optar por girar os arquivos de log com base no tamanho do log e em uma programação, definindo o `-rotate-size` parâmetro e os parâmetros de rotação baseados no tempo em qualquer combinação. Por exemplo: Se `-rotate-size` estiver definido para 10 MB e `-rotate-schedule-minute` estiver definido para 15, os arquivos de log rodam quando o tamanho do arquivo de log atinge 10 MB ou nos 15th minutos de cada hora (o que ocorrer primeiro).

Crie uma configuração de auditoria de arquivos e diretórios em SVMs

Crie a configuração de auditoria

A criação de uma configuração de auditoria de arquivos e diretórios na máquina virtual de storage (SVM) inclui compreender as opções de configuração disponíveis, Planejar a configuração e, em seguida, configurar e ativar a configuração. Em seguida, você pode exibir informações sobre a configuração de auditoria para confirmar se a configuração resultante é a configuração desejada.

Antes de iniciar a auditoria de eventos de arquivo e diretório, crie uma configuração de auditoria na máquina virtual de storage (SVM).

Antes de começar

Se você planeja criar uma configuração de auditoria para o preparo de políticas de acesso central, um servidor SMB deve existir no SVM.

- Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, os eventos de estadiamento da política de acesso central são gerados somente se o Controle de Acesso Dinâmico estiver ativado.

  O Dynamic Access Control é ativado através de uma opção de servidor SMB. Ele não está habilitado por padrão.

- Se os argumentos de um campo em um comando forem inválidos, por exemplo, entradas inválidas para campos, entradas duplicadas e entradas inexistentes, o comando falhará antes da fase de auditoria.

  Tais falhas não geram um Registro de auditoria.

Sobre esta tarefa

Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino não poderá estar no volume raiz.

Passo

1. Usando as informações na Planilha de Planejamento, crie a configuração de auditoria para girar os logs de auditoria com base no tamanho do log ou em uma programação:

Se você quiser girar logs de auditoria…	Digite…
Tamanho do registo	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Uma programação	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Exemplos

O exemplo a seguir cria uma configuração de auditoria que audita operações de arquivo e eventos de logon e logoff SMB (o padrão) usando rotação baseada em tamanho. O formato de log é `EVTX` (o padrão). Os logs são armazenados no `/audit_log` diretório. O limite de tamanho do ficheiro de registo é `200 MB`. Os logs são girados quando atingem 200 MB de tamanho:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

O exemplo a seguir cria uma configuração de auditoria que audita operações de arquivo e eventos de logon e logoff SMB (o padrão) usando rotação baseada em tamanho. O formato de log é `EVTX` (o padrão). Os logs são armazenados no `/cifs_event_logs` diretório. O limite de tamanho do arquivo de log é `100 MB` (o padrão) e o limite de rotação do log é `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

O exemplo a seguir cria uma configuração de auditoria que audita operações de arquivo, eventos de logon e logoff CIFS e eventos de preparação de políticas de acesso central usando rotação baseada em tempo. O

formato de log é `EVTX` (o padrão). Os logs de auditoria são girados mensalmente, às 12:30 horas em todos os dias da semana. O limite de rotação do registo é `5`de :

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Informações relacionadas

- "Habilite a auditoria no SVM"
- "Verifique a configuração de auditoria"

Habilite a auditoria no SVM

Depois de concluir a configuração de auditoria, será necessário habilitar a auditoria na máquina virtual de storage (SVM).

Antes de começar

A configuração de auditoria da SVM já deve existir.

Sobre esta tarefa

Quando uma configuração de descarte de ID de recuperação de desastres da SVM é iniciada pela primeira vez (após a inicialização do SnapMirror ser concluída) e o SVM tiver uma configuração de auditoria, o ONTAP desativa automaticamente a configuração de auditoria. A auditoria é desativada no SVM somente leitura para evitar que os volumes de preparo sejam preenchidos. Você pode ativar a auditoria somente depois que a relação do SnapMirror for interrompida e o SVM for leitura-gravação.

Passos

1. Habilite a auditoria no SVM:

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

Informações relacionadas

- "Crie a configuração de auditoria"
- "Verifique a configuração de auditoria"

Verifique a configuração de auditoria

Depois de concluir a configuração de auditoria, você deve verificar se a auditoria está configurada corretamente e está habilitada.

Passos

1. Verifique a configuração de auditoria:

   ```
   vserver audit show -instance -vserver vserver_name
   ```

O comando a seguir exibe em lista todas as informações de configuração de auditoria da máquina virtual de armazenamento (SVM) VS1:

```
vserver audit show -instance -vserver vs1
```

```
                            Vserver: vs1
                  Auditing state: true
              Log Destination Path: /audit_log
     Categories of Events to Audit: file-ops
                        Log Format: evtx
                Log File Size Limit: 200MB
       Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
     Log Rotation Schedule: Minute: -
                 Rotation Schedules: -
           Log Files Rotation Limit: 0
```

Informações relacionadas

- "Crie a configuração de auditoria"
- "Habilite a auditoria no SVM"

Configurar políticas de auditoria de arquivos e pastas

Configurar políticas de auditoria de arquivos e pastas

Implementar auditoria em eventos de acesso a arquivos e pastas é um processo de duas etapas. Primeiro, você deve criar e habilitar uma configuração de auditoria em máquinas virtuais de storage (SVMs). Em segundo lugar, você deve configurar políticas de auditoria nos arquivos e pastas que deseja monitorar. Você pode configurar políticas de auditoria para monitorar tentativas de acesso bem-sucedidas e com falha.

Você pode configurar políticas de auditoria SMB e NFS. As políticas de auditoria SMB e NFS têm requisitos de configuração e funcionalidades de auditoria diferentes.

Se as políticas de auditoria apropriadas estiverem configuradas, o ONTAP monitora eventos de acesso SMB e NFS conforme especificado nas políticas de auditoria somente se os servidores SMB ou NFS estiverem em execução.

Configurar políticas de auditoria em arquivos e diretórios de estilo de segurança NTFS

Antes de poder auditar operações de arquivo e diretório, você deve configurar políticas de auditoria nos arquivos e diretórios para os quais deseja coletar informações de auditoria. Isso é além de configurar e ativar a configuração de auditoria. Você pode configurar políticas de auditoria NTFS usando a guia Segurança do Windows ou usando a CLI do ONTAP.

Configurando diretivas de auditoria NTFS usando a guia Segurança do Windows

Você pode configurar políticas de auditoria NTFS em arquivos e diretórios usando a guia **Segurança do Windows** na janela Propriedades do Windows. Este é o mesmo método usado ao configurar políticas de auditoria em dados residentes em um cliente Windows, que permite que você use a mesma interface GUI que você está acostumado a usar.

Antes de começar

A auditoria deve ser configurada na máquina virtual de storage (SVM) que contém os dados aos quais você está aplicando as listas de controle de acesso do sistema (SACLs).

Sobre esta tarefa

A configuração de diretivas de auditoria NTFS é feita adicionando entradas a SACLs NTFS que estão associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS. Essas tarefas são tratadas automaticamente pela GUI do Windows. O descritor de segurança pode conter listas de controle de acesso discricionárias (DACLs) para aplicar permissões de acesso a arquivos e pastas, SACLs para auditoria de arquivos e pastas ou SACLs e DACLs.

Para definir políticas de auditoria NTFS usando a guia Segurança do Windows, execute as seguintes etapas em um host do Windows:

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o nome do servidor SMB que contém o compartilhamento, mantendo os dados que deseja auditar e o nome do compartilhamento.

      Você pode especificar o endereço IP da interface de dados para o servidor SMB em vez do nome do servidor SMB.

      Se o nome do servidor SMB for ""SMB_SERVER"" e o compartilhamento for chamado "hare1", você deverá inserir `\\SMB_SERVER\share1`.

   c. Clique em **Finish**.

   A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

3. Selecione o ficheiro ou diretório para o qual pretende ativar o acesso de auditoria.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.
6. Clique em **Avançado**.
7. Selecione a guia **Auditoria**.
8. Execute as ações desejadas:

Se você quiser	Faça o seguinte

Configure a auditoria para um novo usuário ou grupo	a. Clique em **Add**. b. Na caixa Digite o nome do objeto a ser selecionado, digite o nome do usuário ou grupo que deseja adicionar. c. Clique em **OK**.
Remova a auditoria de um usuário ou grupo	a. Na caixa Digite o nome do objeto a ser selecionado, selecione o usuário ou grupo que deseja remover. b. Clique em **Remover**. c. Clique em **OK**. d. Ignore o resto deste procedimento.
Alterar a auditoria para um usuário ou grupo	a. Na caixa Digite o nome do objeto a ser selecionado, selecione o usuário ou grupo que deseja alterar. b. Clique em **Editar**. c. Clique em **OK**.

Se você estiver configurando a auditoria em um usuário ou grupo ou alterando a auditoria em um usuário ou grupo existente, a caixa Entrada de Auditoria para <object> será aberta.

9. Na caixa **aplicar a**, selecione como você deseja aplicar essa entrada de auditoria.

   Pode selecionar uma das seguintes opções:

   - **Esta pasta, subpastas e ficheiros**
   - **Esta pasta e subpastas**
   - **Somente esta pasta**
   - **Esta pasta e ficheiros**
   - **Somente subpastas e arquivos**
   - **Somente subpastas**
   - **Somente arquivos** se você estiver configurando a auditoria em um único arquivo, a caixa **aplicar a** não estará ativa. A configuração da caixa **Apply to** é padrão para **this object only**.

   Como a auditoria exige recursos da SVM, selecione apenas o nível mínimo que forneça os eventos de auditoria que atendam aos seus requisitos de segurança.

10. Na caixa **Access**, selecione o que deseja auditado e se deseja auditar eventos bem-sucedidos, eventos de falha ou ambos.
    - Para auditar eventos bem-sucedidos, selecione a caixa sucesso.
    - Para auditar eventos de falha, selecione a caixa Falha.

      Selecione apenas as ações que você precisa monitorar para atender aos requisitos de segurança. Para obter mais informações sobre esses eventos auditáveis, consulte a documentação do Windows. Você pode auditar os seguintes eventos:

    - * Controle total*

- * Traverse pasta / executar arquivo *
- **Lista de pastas / dados de leitura**
- **Leia atributos**
- **Leia atributos estendidos**
- * Criar arquivos / escrever dados *
- * Criar pastas / anexar dados*
- * Escrever atributos*
- **Escreva atributos estendidos**
- **Excluir subpastas e arquivos**
- **Excluir**
- **Permissões de leitura**
- **Alterar permissões**
- **Assuma a propriedade**

11. Se você não quiser que a configuração de auditoria se propague para arquivos e pastas subsequentes do contentor original, marque a caixa **aplicar essas entradas de auditoria a objetos e/ou contentores dentro desse contentor somente**.
12. Clique em **aplicar**.
13. Depois de terminar de adicionar, remover ou editar entradas de auditoria, clique em **OK**.

    A caixa Entrada Auditoria para <object> fecha.

14. Na caixa **Auditoria**, selecione as configurações de herança para esta pasta.

    Selecione apenas o nível mínimo que fornece os eventos de auditoria que atendem aos seus requisitos de segurança. Você pode escolher uma das seguintes opções:

    - Selecione a caixa incluir entradas de auditoria herdáveis na caixa pai deste objeto.
    - Selecione a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto.
    - Selecione ambas as caixas.
    - Selecione nenhuma das caixas. Se você estiver configurando SACLs em um único arquivo, a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto não estará presente na caixa Auditoria.

15. Clique em **OK**.

    A caixa Auditoria fecha.

Configurar políticas de auditoria NTFS usando a CLI do ONTAP

Você pode configurar políticas de auditoria em arquivos e pastas usando a CLI do ONTAP. Isso permite configurar políticas de auditoria NTFS sem a necessidade de se conetar aos dados usando um compartilhamento SMB em um cliente Windows.

Você pode configurar políticas de auditoria NTFS usando a `vserver security file-directory` família de comandos.

Você só pode configurar SACLs NTFS usando a CLI. A configuração de SACLs NFSv4 não é suportada com esta família de comandos ONTAP. Consulte as páginas de manual para obter mais informações sobre como usar esses comandos para configurar e adicionar SACLs NTFS a arquivos e pastas.

Configurar auditoria para arquivos e diretórios de estilo de segurança UNIX

Você configura a auditoria de arquivos e diretórios de estilo de segurança UNIX adicionando ACEs de auditoria a ACLs NFSv4.x. Isso permite que você monitore determinados eventos de acesso a arquivos NFS e diretórios para fins de segurança.

Sobre esta tarefa

Para NFSv4.x, os ACEs discricionários e do sistema são armazenados na mesma ACL. Eles não são armazenados em DACLs e SACLs separados. Portanto, você deve ter cuidado ao adicionar ACEs de auditoria a uma ACL existente para evitar sobrescrever e perder uma ACL existente. A ordem em que você adiciona os ACEs de auditoria a uma ACL existente não importa.

Passos

1. Recupere a ACL existente para o arquivo ou diretório usando o `nfs4_getfacl` comando ou equivalente.

   Para obter mais informações sobre como manipular ACLs, consulte as páginas de manual do seu cliente NFS.

2. Anexe os ACEs de auditoria desejados.
3. Aplique a ACL atualizada ao arquivo ou diretório usando o `nfs4_setfacl` comando ou equivalente.

Exibir informações sobre políticas de auditoria aplicadas a arquivos e diretórios

Exiba informações sobre políticas de auditoria usando a guia Segurança do Windows

Você pode exibir informações sobre políticas de auditoria que foram aplicadas a arquivos e diretórios usando a guia Segurança na janela Propriedades do Windows. Este é o mesmo método usado para dados que residem em um servidor Windows, que permite que os clientes usem a mesma interface GUI que estão acostumados a usar.

Sobre esta tarefa

A exibição de informações sobre políticas de auditoria aplicadas a arquivos e diretórios permite verificar se você tem as listas de controle de acesso do sistema (SACLs) apropriadas definidas em arquivos e pastas especificados.

Para exibir informações sobre SACLs que foram aplicadas a arquivos e pastas NTFS, execute as etapas a seguir em um host do Windows.

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa de diálogo **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o endereço IP ou o nome do servidor SMB da máquina virtual de armazenamento (SVM) que contém o compartilhamento que contém os dados que deseja auditar e o nome do compartilhamento.

Se o nome do servidor SMB for ""SMB_SERVER"" e o compartilhamento for chamado "hare1", você deverá inserir `\\SMB_SERVER\share1`.

> Você pode especificar o endereço IP da interface de dados para o servidor SMB em vez do nome do servidor SMB.

c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

3. Selecione o arquivo ou diretório para o qual você exibe informações de auditoria.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.
6. Clique em **Avançado**.
7. Selecione a guia **Auditoria**.
8. Clique em **continuar**.

   Abre-se a caixa Auditoria. A caixa **Auditoria de entradas** exibe um resumo de usuários e grupos que têm SACLs aplicados a eles.

9. Na caixa **Auditoria de entradas**, selecione o usuário ou grupo cujas entradas SACL você deseja exibir.
10. Clique em **Editar**.

    A caixa Entrada Auditoria para <object> será aberta.

11. Na caixa **Access**, exiba os SACLs atuais aplicados ao objeto selecionado.
12. Clique em **Cancelar** para fechar a caixa **Entrada de Auditoria para <object>**.
13. Clique em **Cancelar** para fechar a caixa **Auditoria**.

Exibir informações sobre políticas de auditoria NTFS em volumes FlexVol usando a CLI

Você pode exibir informações sobre políticas de auditoria NTFS no FlexVol volumes, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre listas de controle de acesso do sistema. Você pode usar as informações para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

A exibição de informações sobre políticas de auditoria aplicadas a arquivos e diretórios permite verificar se você tem as listas de controle de acesso do sistema (SACLs) apropriadas definidas em arquivos e pastas especificados.

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou pastas cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança NTFS usam apenas as listas de controle de acesso do sistema NTFS (SACLs) para políticas de auditoria.

- Arquivos e pastas em um volume misto de estilo de segurança com segurança efetiva NTFS podem ter políticas de auditoria NTFS aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir tanto o arquivo normal quanto a pasta NFSv4 SACLs e o Storage-Level Access Guard NTFS SACLs.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório fornecido.
- Ao exibir informações de segurança sobre arquivos e pastas com segurança efetiva NTFS, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.

  Arquivos e pastas de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos.

- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.

Passo

1. Exiba as configurações de diretiva de auditoria de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Como uma lista detalhada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações da política de auditoria do caminho `/corp` no SVM VS1. O caminho tem segurança eficaz NTFS. O descritor de segurança NTFS contém uma entrada SACL DE sucesso e uma entrada de sucesso/FALHA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

O exemplo a seguir exibe as informações da política de auditoria do caminho `/datavol1` no SVM VS1. O caminho contém SACLs de arquivo e pasta regulares e SACLs de proteção de acesso em nível de armazenamento.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Maneiras de exibir informações sobre segurança de arquivos e diretivas de auditoria

Você pode usar o caractere curinga (*) para exibir informações sobre segurança de arquivos e políticas de auditoria de todos os arquivos e diretórios em um determinado

caminho ou volume raiz.

O caractere curinga (*) pode ser usado como o último subcomponente de um determinado caminho de diretório abaixo do qual você deseja exibir informações de todos os arquivos e diretórios.

Se você quiser exibir informações de um arquivo ou diretório específico chamado "*", então você precisa fornecer o caminho completo dentro de aspas duplas (" ").

Exemplo

O comando a seguir com o caractere curinga exibe as informações sobre todos os arquivos e diretórios abaixo do caminho `/1/` do SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

O comando a seguir exibe as informações de um arquivo chamado "*" no caminho `/vol1/a` do SVM VS1. O caminho está entre aspas duplas (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Eventos de mudança de CLI que podem ser auditados

CLI alterar eventos que podem ser auditados visão geral

O ONTAP pode auditar certos eventos de mudança de CLI, incluindo certos eventos de compartilhamento de SMB, certos eventos de política de auditoria, determinados eventos de grupo de segurança local, eventos de grupo de usuários locais e eventos de política de autorização. Entender quais eventos de mudança podem ser auditados é útil ao interpretar os resultados dos logs de eventos.

Você pode gerenciar eventos de alteração da CLI de auditoria de máquina virtual de storage (SVM) girando manualmente os logs de auditoria, habilitando ou desativando a auditoria, exibindo informações sobre auditoria de eventos de alterações, modificando eventos de auditoria de alterações e excluindo eventos de alteração de auditoria.

Como administrador, se você executar qualquer comando para alterar a configuração relacionada aos eventos SMB-share, grupo de usuários local, grupo de segurança local, política de autorização e política de auditoria, um Registro será gerado e o evento correspondente será auditado:

Categoria Auditoria	Eventos	IDs de eventos	Execute este comando…
Auditoria Mhost	mudança de política	[4719] Configuração de auditoria alterada	`vserver audit disable

enable	modify`	compartilhamento de arquivos	[5142] a partilha de rede foi adicionada
`vserver cifs share create`	[5143] a partilha de rede foi modificada	`vserver cifs share modify` `vserver cifs share create`	modify
delete` `vserver cifs share add	remove`	[5144] partilha de rede eliminada	`vserver cifs share delete`
Auditoria	conta de utilizador	[4720] usuário local criado	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] utilizador local ativado	`vserver cifs users-and-groups local-user create	modify`	[4724] Reposição da palavra-passe do utilizador local
`vserver cifs users-and-groups local-user set-password`	[4725] Utilizador local desativado	`vserver cifs users-and-groups local-user create	modify`
[4726] utilizador local eliminado	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] alteração do utilizador local	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] Renomear utilizador local	`vserver cifs users-and-groups local-user rename`	grupo de segurança	[4731] Grupo de Segurança local criado
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Grupo de Segurança local eliminado	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Grupo de Segurança local modificado

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] Usuário adicionado ao Grupo local	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] Usuário removido do Grupo local	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	autorização-política-alteração	[4704] Direitos de Usuário atribuídos
`vserver cifs users-and-groups privilege add-privilege`	[4705] Direitos de usuário removidos	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

Gerenciar evento de compartilhamento de arquivos

Quando um evento de compartilhamento de arquivos é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados. Os eventos de compartilhamento de arquivos são gerados quando o compartilhamento de rede SMB é modificado usando `vserver cifs share` comandos relacionados.

Os eventos de compartilhamento de arquivos com as ids de eventos 5142, 5143 e 5144 são gerados quando um compartilhamento de rede SMB é adicionado, modificado ou excluído para o SVM. A configuração de compartilhamento de rede SMB é modificada usando os `cifs share access control create|modify|delete` comandos.

O exemplo a seguir exibe um evento de compartilhamento de arquivos com a ID 5143 é gerado, quando um objeto de compartilhamento chamado 'audit_dest' é criado:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Gerenciar evento de mudança de política de auditoria

Quando um evento de alteração de política de auditoria é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados. Os eventos de alteração de política de auditoria são gerados quando uma diretiva de auditoria é modificada usando `vserver audit` comandos relacionados.

O evento de alteração de política de auditoria com o ID de evento 4719 é gerado sempre que uma política de auditoria é desativada, ativada ou modificada e ajuda a identificar quando um usuário tenta desativar a auditoria para cobrir os trajetos. Ele é configurado por padrão e requer privilégio de diagnóstico para ser desativado.

O exemplo a seguir exibe um evento de mudança de diretiva de auditoria com a ID 4719 gerada, quando uma auditoria é desativada:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Gerenciar evento de conta de usuário

Quando um evento de conta de usuário é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos da conta de usuário com ids de eventos 4720, 4722, 4724, 4725, 4726, 4738 e 4781 são gerados quando um usuário SMB ou NFS local é criado ou excluído do sistema, a conta de usuário local é ativada, desativada ou modificada e a senha de usuário SMB local é redefinida ou alterada. Os eventos de conta de usuário são gerados quando uma conta de usuário é modificada usando `vserver cifs users-and-groups <local user>` comandos e `vserver services name-service <unix user>`.

O exemplo a seguir exibe um evento de conta de usuário com a ID 4720 gerada, quando um usuário SMB local é criado:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

O exemplo a seguir exibe um evento de conta de usuário com a ID 4781 gerada, quando o usuário local SMB criado no exemplo anterior é renomeado:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Gerenciar evento do grupo de segurança

Quando um evento de grupo de segurança é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos de grupo de segurança com ids de eventos 4731, 4732, 4733, 4734 e 4735 são gerados quando um grupo SMB ou NFS local é criado ou excluído do sistema e o usuário local é adicionado ou removido do grupo. Os eventos de grupo de segurança são gerados quando uma conta de usuário é modificada usando `vserver cifs users-and-groups <local-group>` comandos e `vserver services name-service <unix-group>`.

O exemplo a seguir exibe um evento de grupo de segurança com a ID 4731 gerada, quando um grupo de segurança UNIX local é criado:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Gerenciar evento de alteração de política de autorização

Quando o evento de alteração de política de autorização é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos autorização-política-mudança com os ids de evento 4704 e 4705 são gerados sempre que os direitos de autorização são concedidos ou revogados para um usuário SMB e grupo SMB. Os eventos autorização-política-mudança são gerados quando os direitos de autorização são atribuídos ou revogados usando `vserver cifs users-and-groups privilege` comandos relacionados.

O exemplo a seguir exibe um evento de política de autorização com a ID 4704 gerada, quando os direitos de autorização para um grupo de usuários SMB são atribuídos:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Gerenciar configurações de auditoria

Rode manualmente os registos de eventos de auditoria

Antes de poder visualizar os registos de eventos de auditoria, os registos têm de ser convertidos para formatos legíveis pelo utilizador. Se você quiser exibir os logs de eventos de uma máquina virtual de storage específica (SVM) antes que o ONTAP gire automaticamente o log, você pode girar manualmente os logs de eventos de auditoria em uma SVM.

Passo

1. Gire os logs de eventos de auditoria usando o `vserver audit rotate-log` comando.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   O log de eventos de auditoria é salvo no diretório de log de eventos de auditoria SVM com o formato especificado pela configuração de auditoria (`XML`ou `EVTX`) e pode ser visualizado usando o aplicativo apropriado.

Ativar e desativar a auditoria em SVMs

Você pode ativar ou desativar a auditoria em máquinas virtuais de armazenamento (SVMs). Talvez você queira interromper temporariamente a auditoria de arquivos e diretórios desativando a auditoria. Você pode ativar a auditoria a qualquer momento (se houver uma configuração de auditoria).

O que você vai precisar

Antes de habilitar a auditoria na SVM, a configuração de auditoria da SVM já deve existir.

"Crie a configuração de auditoria"

Sobre esta tarefa

A desativação da auditoria não exclui a configuração de auditoria.

Passos

1. Execute o comando apropriado:

Se você quer que a auditoria seja…	Digite o comando…
Ativado	`vserver audit enable -vserver vserver_name`
Desativado	`vserver audit disable -vserver vserver_name`

2. Verifique se a auditoria está no estado desejado:

   `vserver audit show -vserver vserver_name`

Exemplos

O exemplo a seguir permite a auditoria do SVM VS1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
               Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                        Log Format: evtx
                 Log File Size Limit: 100MB
       Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

O exemplo a seguir desativa a auditoria para SVM VS1:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Exibir informações sobre configurações de auditoria

Você pode exibir informações sobre configurações de auditoria. As informações podem ajudá-lo a determinar se a configuração é o que você deseja em vigor para cada SVM. As informações exibidas também permitem verificar se uma configuração de auditoria está ativada.

Sobre esta tarefa

Você pode exibir informações detalhadas sobre configurações de auditoria em todos os SVMs ou pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Se não especificar nenhum dos parâmetros opcionais, é apresentado o seguinte:

- Nome do SVM ao qual a configuração de auditoria se aplica
- O estado de auditoria, que pode ser `true` ou `false`

  Se o estado de auditoria for `true`, a auditoria será ativada. Se o estado de auditoria for `false`, a auditoria será desativada.

- As categorias de eventos a auditar
- O formato do log de auditoria
- O diretório de destino onde o subsistema de auditoria armazena logs de auditoria consolidados e convertidos

Passo

1. Exiba informações sobre a configuração de auditoria usando o `vserver audit show` comando.

   Para obter mais informações sobre como usar o comando, consulte as páginas de manual.

Exemplos

O exemplo a seguir exibe um resumo da configuração de auditoria de todos os SVMs:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

O exemplo a seguir exibe, em forma de lista, todas as informações de configuração de auditoria para todos os SVMs:

```
cluster1::> vserver audit show -instance

                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                         Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
```

Comandos para modificar configurações de auditoria

Se você quiser alterar uma configuração de auditoria, você pode modificar a configuração atual a qualquer momento, incluindo modificar o destino do caminho de log e o formato de log, modificar as categorias de eventos a auditar, como salvar automaticamente arquivos de log e especificar o número máximo de arquivos de log a serem salvos.

Se você quiser…	Use este comando…
Modifique o caminho de destino do log	`vserver audit modify` com o `-destination` parâmetro

Modifique a categoria de eventos para auditoria	`vserver audit modify` com o `-events` parâmetro Para auditar eventos de preparação de políticas de acesso central, a opção servidor SMB de controle de acesso dinâmico (DAC) deve estar ativada na máquina virtual de armazenamento (SVM).
Modifique o formato do log	`vserver audit modify` com o `-format` parâmetro
Ativar gravações automáticas com base no tamanho do ficheiro de registo interno	`vserver audit modify` com o `-rotate-size` parâmetro
Ativar as gravações automáticas com base num intervalo de tempo	`vserver audit modify` com os `-rotate -schedule-month` parâmetros , `-rotate -schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour` e `-rotate -schedule-minute`
Especificar o número máximo de ficheiros de registo guardados	`vserver audit modify` com o `-rotate-limit` parâmetro

Excluir uma configuração de auditoria

Se você não quiser mais auditar eventos de arquivo e diretório na máquina virtual de storage (SVM) e não quiser manter uma configuração de auditoria na SVM, é possível excluir a configuração de auditoria.

Passos

1. Desative a configuração de auditoria:

   ```
   vserver audit disable -vserver vserver_name

   vserver audit disable -vserver vs1
   ```

2. Excluir a configuração de auditoria:

   ```
   vserver audit delete -vserver vserver_name

   vserver audit delete -vserver vs1
   ```

Entenda as implicações de reverter o cluster

Se você pretende reverter o cluster, deve estar ciente do processo de reversão que o ONTAP segue quando houver máquinas virtuais de storage (SVMs) habilitadas para

auditoria no cluster. Você deve tomar certas ações antes de reverter.

Revertendo para uma versão do ONTAP que não suporte a auditoria de eventos de logon e logoff SMB e eventos de preparação de políticas de acesso central

O suporte para auditoria de eventos de logon e logoff SMB e para eventos de preparação de políticas de acesso central começa com o Clustered Data ONTAP 8.3. Se você estiver revertendo para uma versão do ONTAP que não ofereça suporte a esses tipos de eventos e tiver configurações de auditoria que monitorem esses tipos de eventos, será necessário alterar a configuração de auditoria desses SVMs habilitados para auditoria antes de reverter. Você deve modificar a configuração para que apenas eventos de arquivo operacional sejam auditados.

Solucionar problemas de volume de auditoria e preparação

Problemas podem surgir quando não houver espaço suficiente nos volumes de teste ou no volume que contém os logs de eventos de auditoria. Se não houver espaço suficiente, novos Registros de auditoria não podem ser criados, o que impede que os clientes acessem dados e as solicitações de acesso falhem. Você deve saber como solucionar e resolver esses problemas de espaço de volume.

Solucionar problemas de espaço relacionados aos volumes de log de eventos

Se os volumes contendo arquivos de log de eventos ficarem sem espaço, a auditoria não poderá converter Registros de log em arquivos de log. Isso resulta em falhas de acesso do cliente. Você deve saber como solucionar problemas de espaço relacionados aos volumes de log de eventos.

- Os administradores de cluster e máquina virtual de storage (SVM) podem determinar se há espaço de volume insuficiente exibindo informações sobre o volume e o uso e a configuração agregados.
- Se houver espaço insuficiente nos volumes que contêm logs de eventos, os administradores de SVM e cluster poderão resolver os problemas de espaço removendo alguns dos arquivos de log de eventos ou aumentando o tamanho do volume.

> Se o agregado que contém o volume do log de eventos estiver cheio, o tamanho do agregado deve ser aumentado antes que você possa aumentar o tamanho do volume. Somente um administrador de cluster pode aumentar o tamanho de um agregado.

- O caminho de destino para os arquivos de log de eventos pode ser alterado para um diretório em outro volume, modificando a configuração de auditoria.

> O acesso aos dados é negado nos seguintes casos:
>
> - O diretório de destino é excluído.
> - O limite de arquivo em um volume, que hospeda o diretório de destino, atinge seu nível máximo.

Saiba mais sobre:

- "Como visualizar informações sobre volumes e aumentar o tamanho do volume".
- "Como visualizar informações sobre agregados e gerenciar agregados".

Solucionar problemas de espaço relacionados aos volumes de teste

Se algum dos volumes que contém arquivos de teste para a máquina virtual de armazenamento (SVM) ficar sem espaço, a auditoria não poderá gravar Registros de log em arquivos de teste. Isso resulta em falhas de acesso do cliente. Para solucionar esse problema, você precisa determinar se algum dos volumes de teste usados no SVM está cheio exibindo informações sobre o uso de volume.

Se o volume que contém os arquivos de log de eventos consolidados tiver espaço suficiente, mas ainda houver falhas de acesso do cliente devido a espaço insuficiente, os volumes de teste podem estar fora do espaço. O administrador do SVM deve entrar em Contato com você para determinar se os volumes de teste que contêm arquivos de teste para o SVM têm espaço insuficiente. O subsistema de auditoria gera um evento EMS se os eventos de auditoria não puderem ser gerados devido a espaço insuficiente em um volume de teste. É apresentada a seguinte mensagem: `No space left on device`. Somente você pode exibir informações sobre volumes de teste; os administradores do SVM não podem.

Todos os nomes de volume de estadiamento começam com `MDV_aud_` seguido pelo UUID do agregado que contém esse volume de estadiamento. O exemplo a seguir mostra quatro volumes de sistema no SVM admin, que foram criados automaticamente quando uma configuração de auditoria de serviços de arquivo foi criada para um data SVM no cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

Se não houver espaço suficiente nos volumes de teste, você poderá resolver os problemas de espaço aumentando o tamanho do volume.

> Se o agregado que contém o volume de estadiamento estiver cheio, o tamanho do agregado deverá ser aumentado antes de poder aumentar o tamanho do volume. Somente você pode aumentar o tamanho de um agregado. Os administradores de SVM não podem.

Se um ou mais agregados tiverem um espaço disponível inferior a 2GB TB (no ONTAP 9.14,1 e anterior) ou 5GB TB (começando com o ONTAP 9.15,1), a criação da auditoria SVM falhará. Quando a criação da auditoria SVM falhar, os volumes de teste criados são excluídos.

Use o FPolicy para monitoramento e gerenciamento de arquivos em SVMs

Entenda o FPolicy

Quais são as duas partes da solução FPolicy

O FPolicy é uma estrutura de notificação de acesso a arquivos usada para monitorar e gerenciar eventos de acesso a arquivos em máquinas virtuais de armazenamento (SVMs) por meio de soluções de parceiros. Com as soluções do parceiro, você lida com vários casos de uso, como conformidade e governança de dados, proteção de ransomware e mobilidade de dados.

As soluções de parceiros incluem as soluções de 3rd partes compatíveis com a NetApp e os produtos NetApp para carga de trabalho Segurança e Cloud Data Sense.

Existem duas partes para uma solução FPolicy. A estrutura FPolicy do ONTAP gerencia atividades no cluster e envia notificações para o aplicativo de parceiros (também conhecido como servidores FPolicy externos). Servidores FPolicy externos processam notificações enviadas pelo ONTAP FPolicy para atender casos de uso do cliente.

A estrutura ONTAP cria e mantém a configuração FPolicy, monitora eventos de arquivo e envia notificações para servidores FPolicy externos. O ONTAP FPolicy fornece a infraestrutura que permite a comunicação entre servidores FPolicy externos e nós de máquina virtual de storage (SVM).

A estrutura FPolicy coneta-se a servidores FPolicy externos e envia notificações para determinados eventos do sistema de arquivos para os servidores FPolicy quando esses eventos ocorrem como resultado do acesso do cliente. Os servidores FPolicy externos processam as notificações e enviam respostas de volta para o nó. O que acontece como resultado do processamento de notificações depende do aplicativo e se a comunicação entre o nó e os servidores externos é assíncrona ou síncrona.

Quais são as notificações síncronas e assíncronas

O FPolicy envia notificações para servidores FPolicy externos através da interface FPolicy. As notificações são enviadas em modo síncrono ou assíncrono. O modo de notificação determina o que o ONTAP faz depois de enviar notificações para servidores FPolicy.

- **Notificações assíncronas**

  Com notificações assíncronas, o nó não espera por uma resposta do servidor FPolicy, que aumenta a taxa de transferência geral do sistema. Esse tipo de notificação é adequado para aplicativos em que o servidor FPolicy não exige que qualquer ação seja tomada como resultado da avaliação da notificação. Por exemplo, notificações assíncronas são usadas quando o administrador da máquina virtual de storage (SVM) deseja monitorar e auditar a atividade de acesso a arquivos.

  Se um servidor FPolicy que opera no modo assíncrono sofrer uma interrupção na rede, as notificações FPolicy geradas durante a interrupção serão armazenadas no nó de storage. Quando o servidor FPolicy volta online, ele é alertado das notificações armazenadas e pode buscá-las a partir do nó de armazenamento. O período de tempo em que as notificações podem ser armazenadas durante uma interrupção é configurável até 10 minutos.

A partir do ONTAP 9.14,1, o FPolicy permite configurar um armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

- **Notificações síncronas**

  Quando configurado para ser executado no modo síncrono, o servidor FPolicy deve reconhecer todas as notificações antes que a operação do cliente possa continuar. Este tipo de notificação é utilizado quando uma ação é necessária com base nos resultados da avaliação da notificação. Por exemplo, as notificações síncronas são usadas quando o administrador da SVM deseja permitir ou negar solicitações com base nos critérios especificados no servidor FPolicy externo.

Aplicações síncronas e assíncronas

Existem muitos usos possíveis para aplicativos FPolicy, tanto assíncronos quanto síncronos.

Aplicações assíncronas são aquelas em que o servidor FPolicy externo não altera o acesso a arquivos ou diretórios nem modifica dados na máquina virtual de armazenamento (SVM). Por exemplo:

- Acesso a arquivos e Registro de auditoria
- Gerenciamento de recursos de storage

Os aplicativos síncronos são aqueles em que o acesso aos dados é alterado ou os dados são modificados pelo servidor FPolicy externo. Por exemplo:

- Gerenciamento de cota
- Bloqueio de acesso a arquivos
- Arquivamento de arquivos e gerenciamento de armazenamento hierárquico
- Serviços de criptografia e descriptografia
- Serviços de compressão e descompressão

Armazenamentos persistentes de FPolicy

Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente. A partir do ONTAP 9.14,1, é possível configurar um armazenamento persistente FPolicy para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

Esta funcionalidade só está disponível no modo externo FPolicy. A aplicação de parceiro que você usa precisa para dar suporte a esse recurso. Você deve trabalhar com seu parceiro para garantir que essa configuração do FPolicy seja suportada.

A partir do ONTAP 9.15,1, a configuração de armazenamento persistente do FPolicy é simplificada. O `persistent-store create` comando automatiza a criação de volume para o SVM e configura o volume com as práticas recomendadas de armazenamento persistente.

Para obter mais informações sobre as práticas recomendadas de armazenamento persistente, "Requisitos,

considerações e práticas recomendadas para configurar o FPolicy"consulte .

Para obter informações sobre como adicionar armazenamentos persistentes, "Crie armazenamentos persistentes"consulte .

Tipos de configuração FPolicy

Existem dois tipos básicos de configuração FPolicy. Uma configuração usa servidores FPolicy externos para processar e agir mediante notificações. A outra configuração não usa servidores FPolicy externos; em vez disso, ele usa o servidor FPolicy interno e nativo do ONTAP para bloqueio de arquivos simples com base em extensões.

- * Configuração externa do servidor FPolicy*

  A notificação é enviada para o servidor FPolicy, que exibe a solicitação e aplica regras para determinar se o nó deve permitir a operação do arquivo solicitado. Para políticas síncronas, o servidor FPolicy envia uma resposta ao nó para permitir ou bloquear a operação de arquivo solicitada.

- * Configuração nativa do servidor FPolicy*

  A notificação é rastreada internamente. A solicitação é permitida ou negada com base nas configurações de extensão de arquivo configuradas no escopo FPolicy.

  Nota: As solicitações de extensão de arquivo negadas não são registradas.

Quando criar uma configuração FPolicy nativa

As configurações nativas de FPolicy usam o mecanismo interno de FPolicy do ONTAP para monitorar e bloquear operações de arquivos com base na extensão do arquivo. Esta solução não requer servidores FPolicy externos (servidores FPolicy). O uso de uma configuração de bloqueio de arquivos nativa é apropriado quando essa solução simples é tudo o que é necessário.

O bloqueio de arquivos nativos permite monitorar quaisquer operações de arquivos que correspondam a eventos de operação e filtragem configurados e, em seguida, negar acesso a arquivos com extensões específicas. Esta é a configuração padrão.

Esta configuração fornece um meio de bloquear o acesso a arquivos com base apenas na extensão do arquivo. Por exemplo, para bloquear arquivos que contêm `mp3` extensões, configure uma política para fornecer notificações para determinadas operações com extensões de arquivo de destino `mp3` do . A política é configurada para negar `mp3` solicitações de arquivos para operações que geram notificações.

O seguinte se aplica a configurações nativas de FPolicy:

- O mesmo conjunto de filtros e protocolos que são suportados pela triagem de arquivos baseada no servidor FPolicy também são suportados para bloqueio de arquivos nativos.
- O bloqueio de arquivos nativo e os aplicativos de triagem de arquivos baseados no servidor FPolicy podem ser configurados ao mesmo tempo.

  Para fazer isso, você pode configurar duas políticas FPolicy separadas para a máquina virtual de armazenamento (SVM), com uma configurada para bloqueio de arquivos nativos e uma configurada para triagem de arquivos baseada no servidor FPolicy.

- O recurso de bloqueio de arquivos nativo somente exibe arquivos com base nas extensões e não no

conteúdo do arquivo.

- No caso de links simbólicos, o bloqueio de arquivos nativos usa a extensão de arquivo do arquivo raiz.

Saiba mais "FPolicy: Bloqueio de arquivos nativos"sobre o .

Quando criar uma configuração que use servidores FPolicy externos

As configurações FPolicy que usam servidores FPolicy externos para processar e gerenciar notificações fornecem soluções robustas para casos de uso em que mais do que simples bloqueio de arquivos com base na extensão de arquivo é necessário.

Você deve criar uma configuração que use servidores FPolicy externos quando quiser fazer coisas como monitorar e gravar eventos de acesso a arquivos, fornecer serviços de cota, executar bloqueio de arquivos com base em critérios diferentes de extensões de arquivo simples, fornecer serviços de migração de dados usando aplicativos de gerenciamento de storage hierárquico ou fornecer um conjunto refinado de políticas que monitoram apenas um subconjunto de dados na máquina virtual de armazenamento (SVM).

Funções que os componentes do cluster desempenham com a implementação do FPolicy

O cluster, as máquinas virtuais de armazenamento contido (SVMs) e os LIFs de dados desempenham um papel na implementação de FPolicy.

- **cluster**

  O cluster contém a estrutura de gerenciamento FPolicy e mantém e gerencia informações sobre todas as configurações do FPolicy no cluster.

- **SVM**

  Uma configuração de FPolicy é definida no nível da SVM. O escopo da configuração é o SVM, e só opera com recursos do SVM. Uma configuração do SVM não pode monitorar e enviar notificações de solicitações de acesso a arquivos feitas para dados residentes em outro SVM.

  As configurações de FPolicy podem ser definidas no SVM do administrador. Depois que as configurações são definidas no SVM de administrador, elas podem ser vistas e usadas em todos os SVMs.

- **LIFs de dados**

  As conexões com os servidores FPolicy são feitas por meio de LIFs de dados pertencentes ao SVM com a configuração FPolicy. Os LIFs de dados usados para essas conexões podem falhar da mesma maneira que os LIFs de dados usados para acesso normal ao cliente.

Como o FPolicy funciona com servidores FPolicy externos

Depois que o FPolicy é configurado e ativado na máquina virtual de storage (SVM), o FPolicy é executado em todos os nós nos quais o SVM participa. A FPolicy é responsável por estabelecer e manter conexões com servidores FPolicy externos (servidores FPolicy), processamento de notificações e gerenciamento de mensagens de notificação de e para servidores FPolicy.

Além disso, como parte do gerenciamento de conexão, a FPolicy tem as seguintes responsabilidades:

- Garante que a notificação de arquivos flua através do LIF correto para o servidor FPolicy.

- Garante que, quando vários servidores FPolicy estão associados a uma política, o balanceamento de carga é feito ao enviar notificações para os servidores FPolicy.
- Tenta restabelecer a ligação quando uma ligação a um servidor FPolicy é interrompida.
- Envia as notificações para servidores FPolicy em uma sessão autenticada.
- Gerencia a conexão de dados de leitura de passagem estabelecida pelo servidor FPolicy para atender as solicitações do cliente quando a leitura de passagem estiver ativada.

Como os canais de controle são usados para comunicação FPolicy

O FPolicy inicia uma conexão de canal de controle com um servidor FPolicy externo a partir das LIFs de dados de cada nó que participa de uma máquina virtual de armazenamento (SVM). O FPolicy usa canais de controle para transmitir notificações de arquivos; portanto, um servidor FPolicy pode ver várias conexões de canal de controle com base na topologia da SVM.

Como os canais privilegiados de acesso a dados são usados para comunicação síncrona

Com casos de uso síncronos, o servidor FPolicy acessa dados que residem na máquina virtual de storage (SVM) por meio de um caminho de acesso privilegiado aos dados. O acesso através do caminho privilegiado expõe o sistema de arquivos completo ao servidor FPolicy. Ele pode acessar arquivos de dados para coletar informações, digitalizar arquivos, ler arquivos ou escrever em arquivos.

Como o servidor FPolicy externo pode acessar todo o sistema de arquivos a partir da raiz do SVM por meio do canal de dados privilegiado, a conexão de canal de dados privilegiado deve estar segura.

Como as credenciais de conexão FPolicy são usadas com canais de acesso a dados privilegiados

O servidor FPolicy faz conexões de acesso privilegiado a dados para nós de cluster usando uma credencial de usuário específica do Windows que é salva com a configuração FPolicy. SMB é o único protocolo suportado para fazer uma conexão de canal de acesso a dados privilegiada.

Se o servidor FPolicy exigir acesso privilegiado a dados, as seguintes condições devem ser atendidas:

- Uma licença SMB deve estar ativada no cluster.
- O servidor FPolicy deve ser executado sob as credenciais configuradas na configuração FPolicy.

Ao fazer uma conexão de canal de dados, o FPolicy usa a credencial para o nome de usuário especificado do Windows. O acesso aos dados é feito através do administrador Share ONTAP_ADMIN.

O que significa conceder credenciais de super usuário para acesso privilegiado a dados

O ONTAP usa a combinação do endereço IP e da credencial do usuário configurada na configuração FPolicy para conceder credenciais de super usuário ao servidor FPolicy.

O status de super usuário concede o seguinte Privileges quando o servidor FPolicy acessa dados:

- Evite verificações de permissão

  O usuário evita verificações de arquivos e acesso a diretórios.

- Privileges de bloqueio especial

  O ONTAP permite ler, gravar ou modificar o acesso a qualquer arquivo, independentemente dos bloqueios existentes. Se o servidor FPolicy pegar bloqueios de intervalo de bytes no arquivo, isso resulta na remoção imediata de bloqueios existentes no arquivo.

- Ignorar quaisquer verificações de FPolicy

  O Access não gera nenhuma notificação FPolicy.

Como a FPolicy gerencia o processamento de políticas

Pode haver várias políticas de FPolicy atribuídas à sua máquina virtual de storage (SVM), cada uma com uma prioridade diferente. Para criar uma configuração de FPolicy apropriada no SVM, é importante entender como o FPolicy gerencia o processamento de políticas.

Cada solicitação de acesso ao arquivo é inicialmente avaliada para determinar quais políticas estão monitorando esse evento. Se for um evento monitorado, as informações sobre o evento monitorado junto com as políticas de interesse são passadas para a FPolicy, onde é avaliado. Cada política é avaliada por ordem da prioridade atribuída.

Você deve considerar as seguintes recomendações ao configurar políticas:

- Quando você quiser que uma política seja sempre avaliada antes de outras políticas, configure essa política com uma prioridade mais alta.
- Se o sucesso da operação de acesso a arquivos solicitados em um evento monitorado for um pré-requisito para uma solicitação de arquivo que é avaliada em relação a outra política, dê prioridade à política que controla o sucesso ou falha da operação do primeiro arquivo.

  Por exemplo, se uma diretiva gerencia a funcionalidade de arquivamento e restauração de arquivos FPolicy e uma segunda diretiva gerencia as operações de acesso de arquivos no arquivo on-line, a política que gerencia a restauração de arquivos deve ter uma prioridade maior para que o arquivo seja restaurado antes que a operação gerenciada pela segunda diretiva possa ser permitida.

- Se você quiser que todas as políticas que possam ser aplicadas a uma operação de acesso a arquivos sejam avaliadas, dê prioridade menor às políticas síncronas.

Você pode reordenar as prioridades de política para políticas existentes modificando o número de sequência de políticas. No entanto, para que o FPolicy avalie as políticas com base na ordem de prioridade modificada, você deve desativar e reativar a política com o número de sequência modificado.

Qual é o processo de comunicação do servidor FPolicy nó para externo

Para Planejar adequadamente a configuração do FPolicy, você deve entender o que é o processo de comunicação do servidor FPolicy de nó para externo.

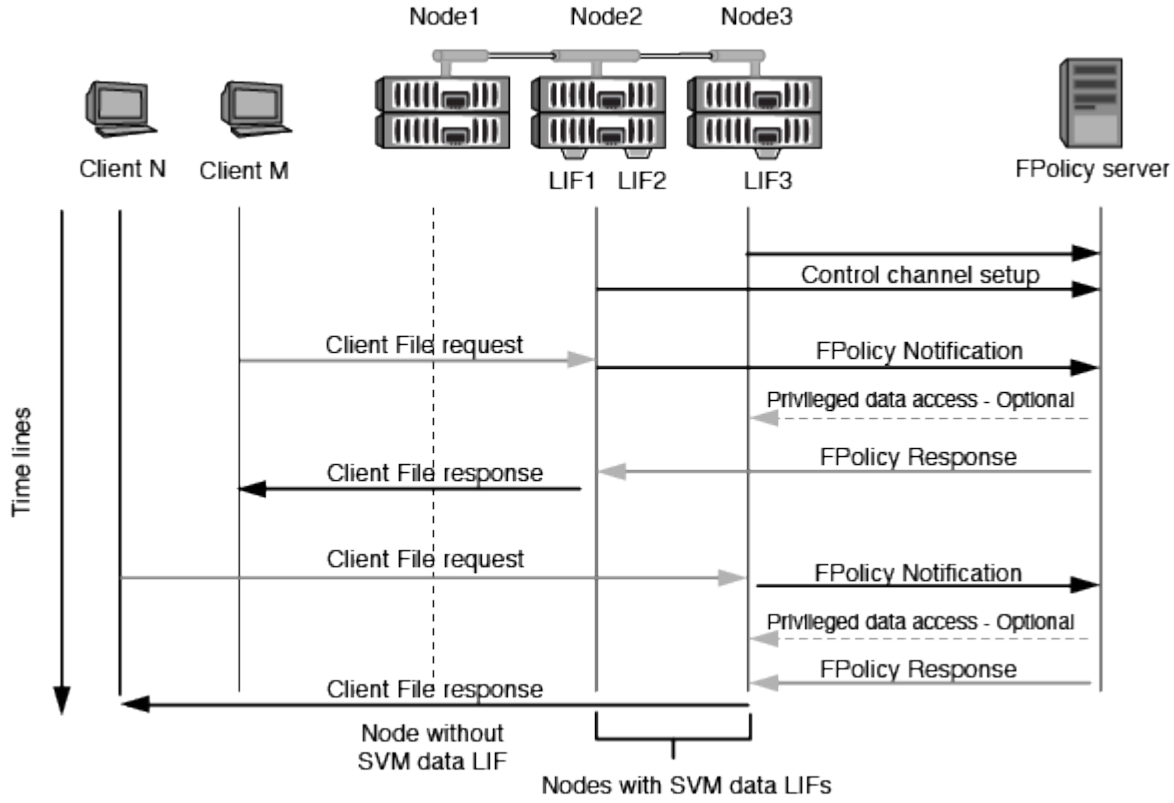
Cada nó que participa de cada máquina virtual de armazenamento (SVM) inicia uma conexão com um servidor FPolicy externo (servidor FPolicy) usando TCP/IP. As conexões com os servidores FPolicy são configuradas usando LIFs de dados de nó; portanto, um nó participante pode configurar uma conexão somente se o nó tiver um LIF de dados operacional para o SVM.

Cada processo de FPolicy nos nós participantes tenta estabelecer uma conexão com o servidor FPolicy quando a diretiva está ativada. Ele usa o endereço IP e a porta do mecanismo externo FPolicy especificado na configuração da política.

A conexão estabelece um canal de controle de cada um dos nós participantes de cada SVM para o servidor FPolicy por meio do data LIF. Além disso, se os endereços de LIF de dados IPv4 e IPv6 estiverem presentes no mesmo nó participante, o FPolicy tentará estabelecer conexões para IPv4 e IPv6. Portanto, em um cenário em que o SVM se estende por vários nós ou se ambos os endereços IPv4 e IPv6 estiverem presentes, o servidor FPolicy deve estar pronto para várias solicitações de configuração de canal de controle do cluster

após a diretiva FPolicy ser ativada no SVM.

Por exemplo, se um cluster tiver três nós - Node1, Node2 e Node3 - e os LIFs de dados SVM estiverem espalhados por apenas Node2 e Node3, os canais de controle serão iniciados apenas a partir de Node2 e Node3, independentemente da distribuição dos volumes de dados. Digamos que o Node2 tem duas LIFs de dados - LIF1 e LIF2 - que pertencem ao SVM e que a conexão inicial é de LIF1. Se o LIF1 falhar, o FPolicy tentará estabelecer um canal de controle a partir do LIF2.



Como o FPolicy gerencia a comunicação externa durante a migração de LIF ou failover

As LIFs de dados podem ser migradas para portas de dados no mesmo nó ou para portas de dados em um nó remoto.

Quando um LIF de dados falha ou é migrado, uma nova conexão de canal de controle é feita para o servidor FPolicy. O FPolicy pode, então, tentar novamente solicitações de clientes SMB e NFS que expiraram, com o resultado de novas notificações serem enviadas para os servidores FPolicy externos. O nó rejeita as respostas do servidor FPolicy às solicitações SMB e NFS originais e com tempo limite.

Como o FPolicy gerencia a comunicação externa durante o failover de nó

Se o nó do cluster que hospeda as portas de dados usadas para comunicação FPolicy falhar, o ONTAP rompe a conexão entre o servidor FPolicy e o nó.

O impactos do failover de cluster no servidor FPolicy pode ser atenuado configurando a política de failover para migrar a porta de dados usada na comunicação FPolicy para outro nó ativo. Após a conclusão da migração, uma nova conexão é estabelecida usando a nova porta de dados.

Se a política de failover não estiver configurada para migrar a porta de dados, o servidor FPolicy deverá aguardar que o nó com falha apareça. Depois que o nó estiver ativo, uma nova conexão será iniciada a partir desse nó com um novo Session ID.

O servidor FPolicy deteta conexões quebradas com a mensagem do protocolo keep-alive. O tempo limite para a purga do Session ID é determinado ao configurar o FPolicy. O limite de tempo de espera predefinido é de dois minutos.

Como os serviços do FPolicy funcionam nos namespaces do SVM

O ONTAP fornece um namespace unificado de máquina virtual de storage (SVM). Os volumes no cluster são Unidos por junções para fornecer um único sistema de arquivos lógico. O servidor FPolicy está ciente da topologia do namespace e fornece serviços FPolicy em todo o namespace.

O namespace é específico e contido no SVM. Portanto, você pode ver o namespace somente no contexto SVM. Os namespaces têm as seguintes caraterísticas:

- Existe um namespace único em cada SVM, com a raiz do namespace sendo o volume raiz, representado no namespace como barra (/).
- Todos os outros volumes têm pontos de junção abaixo da raiz (/).
- Junções de volume são transparentes para os clientes.
- Uma única exportação de NFS pode fornecer acesso ao namespace completo. Caso contrário, as políticas de exportação podem exportar volumes específicos.
- Compartilhamentos SMB podem ser criados no volume ou em qtrees dentro do volume, ou em qualquer diretório dentro do namespace.
- A arquitetura do namespace é flexível.

  Exemplos de arquiteturas de namespace típicas são os seguintes:

  - Um namespace com um único ramo fora da raiz
  - Um namespace com vários ramificações fora da raiz
  - Um namespace com vários volumes não ramificados fora da raiz

Como o FPolicy passa-leitura melhora a usabilidade para o gerenciamento hierárquico de armazenamento

A passagem-leitura permite que o servidor FPolicy (funcionando como servidor de gerenciamento de armazenamento hierárquico (HSM)) forneça acesso de leitura a arquivos off-line sem ter que recuperar o arquivo do sistema de armazenamento secundário para o sistema de armazenamento primário.

Quando um servidor FPolicy é configurado para fornecer HSM a arquivos residentes em um servidor SMB, a migração de arquivos baseada em políticas ocorre onde os arquivos são armazenados off-line no armazenamento secundário e apenas um arquivo stub permanece no armazenamento primário. Mesmo que um arquivo stub apareça como um arquivo normal para os clientes, ele é na verdade um arquivo esparso que é do mesmo tamanho do arquivo original. O arquivo esparso tem o bit off-line SMB definido e aponta para o arquivo real que foi migrado para o armazenamento secundário.

Normalmente, quando uma solicitação de leitura para um arquivo off-line é recebida, o conteúdo solicitado deve ser recuperado de volta para o armazenamento primário e, em seguida, acessado através do armazenamento primário. A necessidade de recuperar dados de volta ao armazenamento primário tem vários efeitos indesejáveis. Entre os efeitos indesejáveis está o aumento da latência das solicitações do cliente

causado pela necessidade de recuperar o conteúdo antes de responder à solicitação e o aumento do consumo de espaço necessário para os arquivos recuperados no armazenamento primário.

O FPolicy Passthrough-read permite que o servidor HSM (o servidor FPolicy) forneça acesso de leitura a arquivos offline migrados sem ter que recuperar o arquivo do sistema de armazenamento secundário para o sistema de armazenamento primário. Em vez de recuperar os arquivos de volta ao armazenamento primário, as solicitações de leitura podem ser atendidas diretamente do armazenamento secundário.

> O descarregamento de cópia (ODX) não é suportado com a operação de passagem-leitura FPolicy.

A passagem-leitura melhora a usabilidade, fornecendo os seguintes benefícios:

- As solicitações de leitura podem ser atendidas mesmo que o armazenamento primário não tenha espaço suficiente para recuperar os dados solicitados de volta ao armazenamento primário.
- Melhor gerenciamento de capacidade e desempenho quando um surto de recuperação de dados pode ocorrer, como se um script ou uma solução de backup precisar acessar muitos arquivos off-line.
- As solicitações de leitura de arquivos off-line em cópias Snapshot podem ser atendidas.

  Como as cópias Snapshot são somente leitura, o servidor FPolicy não pode restaurar o arquivo original se o arquivo stub estiver localizado em uma cópia Snapshot. Usar a passagem-leitura elimina esse problema.

- As políticas podem ser configuradas para controlar quando as solicitações de leitura são atendidas por meio do acesso ao arquivo no armazenamento secundário e quando o arquivo off-line deve ser recuperado para o armazenamento primário.

  Por exemplo, uma política pode ser criada no servidor HSM que especifica o número de vezes que o arquivo off-line pode ser acessado em um período de tempo especificado antes que o arquivo seja migrado de volta para o armazenamento primário. Este tipo de política evita a memorização de ficheiros que raramente são acedidos.

Como as solicitações de leitura são gerenciadas quando a passagem-leitura FPolicy está ativada

Você deve entender como as solicitações de leitura são gerenciadas quando o FPolicy Passthrough-READ está habilitado para que você possa configurar de forma otimizada a conetividade entre a máquina virtual de armazenamento (SVM) e os servidores FPolicy.

Quando a leitura de passagem FPolicy está ativada e o SVM recebe uma solicitação para um arquivo off-line, o FPolicy envia uma notificação para o servidor FPolicy (servidor HSM) por meio do canal de conexão padrão.

Após receber a notificação, o servidor FPolicy lê os dados do caminho do arquivo enviado na notificação e envia os dados solicitados para o SVM por meio da conexão de dados privilegiados de leitura de passagem estabelecida entre o SVM e o servidor FPolicy.

Depois que os dados são enviados, o servidor FPolicy responde à solicitação de leitura como uma PERMISSÃO ou NEGAÇÃO. Com base se a solicitação de leitura é permitida ou negada, o ONTAP envia as informações solicitadas ou envia uma mensagem de erro ao cliente.

Planeie a configuração FPolicy

Requisitos, considerações e práticas recomendadas para configurar o FPolicy

Antes de criar e configurar configurações FPolicy em suas máquinas virtuais de

armazenamento (SVMs), você precisa estar ciente de certos requisitos, considerações e práticas recomendadas para configurar o FPolicy.

Os recursos de FPolicy são configurados por meio da interface de linha de comando (CLI) ou por meio de APIs REST.

Requisitos para configurar FPolicy

Antes de configurar e ativar o FPolicy na máquina virtual de storage (SVM), você precisa estar ciente de certos requisitos.

- Todos os nós no cluster devem estar executando uma versão do ONTAP que suporte FPolicy.
- Se você não estiver usando o mecanismo FPolicy nativo do ONTAP, você deve ter servidores FPolicy externos instalados.
- Os servidores FPolicy devem ser instalados em um servidor acessível a partir das LIFs de dados do SVM onde as políticas FPolicy estão ativadas.

> A partir do ONTAP 9.8, o ONTAP fornece um serviço de LIF cliente para conexões FPolicy de saída com a adição `data-fpolicy-client` do serviço. "Saiba mais sobre LIFs e políticas de serviço".

- O endereço IP do servidor FPolicy deve ser configurado como um servidor primário ou secundário na configuração do mecanismo externo da política FPolicy.
- Se os servidores FPolicy acessarem dados em um canal de dados privilegiado, os seguintes requisitos adicionais devem ser atendidos:
  - O SMB deve ser licenciado no cluster.

    O acesso privilegiado a dados é realizado usando conexões SMB.
  - Uma credencial de usuário deve ser configurada para acessar arquivos pelo canal de dados privilegiado.
  - O servidor FPolicy deve ser executado sob as credenciais configuradas na configuração FPolicy.
  - Todos os LIFs de dados usados para se comunicar com os servidores FPolicy devem ser configurados para ter `cifs` como um dos protocolos permitidos.

    Isso inclui os LIFs usados para conexões de passagem-leitura.

Práticas recomendadas e recomendações ao configurar o FPolicy

Ao configurar o FPolicy em máquinas virtuais de armazenamento (SVMs), familiarize-se com as práticas recomendadas e recomendações gerais de configuração para garantir que sua configuração do FPolicy forneça desempenho de monitoramento robusto e resultados que atendam aos seus requisitos.

Para diretrizes específicas relacionadas a desempenho, dimensionamento e configuração, trabalhe com seu aplicativo de parceiro FPolicy.

Armazenamentos persistentes

A partir do ONTAP 9.14,1, o FPolicy permite configurar um armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para

reduzir a latência do cliente. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

- Antes de usar a funcionalidade de armazenamento persistente, certifique-se de que as aplicações de parceiros suportem esta configuração.
- Você precisa de um armazenamento persistente para cada SVM em que o FPolicy esteja ativado.
  - Apenas um armazenamento persistente pode ser configurado em cada SVM. Esse único armazenamento persistente precisa ser usado em todas as configurações de FPolicy nesse SVM, mesmo que as políticas sejam de parceiros diferentes.
- ONTAP 9.15,1 ou posterior:
  - O armazenamento persistente, seu volume e sua configuração de volume são tratados automaticamente quando você cria o armazenamento persistente.
- ONTAP 9.14,1:
  - O armazenamento persistente, seu volume e sua configuração de volume são manipulados manualmente.
- Crie o volume de armazenamento persistente no nó com LIFs que esperam que o tráfego máximo seja monitorado pelo FPolicy.
  - ONTAP 9.15,1 ou posterior: Os volumes são criados e configurados automaticamente durante a criação do armazenamento persistente.
  - ONTAP 9.14,1: Os administradores de cluster precisam criar e configurar um volume para o armazenamento persistente em cada SVM em que o FPolicy está ativado.
- Se as notificações acumuladas no armazenamento persistente excederem o tamanho do volume provisionado, o FPolicy começa a deixar cair a notificação recebida com mensagens EMS apropriadas.
  - ONTAP 9.15,1 ou posterior: Além do `size` parâmetro, o `autosize-mode` parâmetro pode ajudar o volume a crescer ou diminuir em resposta à quantidade de espaço usado.
  - ONTAP 9.14,1: O `size` parâmetro é configurado durante a criação do volume para fornecer um limite máximo.
- Defina a política de instantâneos como `none` para o volume de armazenamento persistente em vez `default` de . Isso serve para garantir que não haja restauração acidental do snapshot levando à perda de eventos atuais e para evitar possível processamento de eventos duplicados.
  - ONTAP 9.15,1 ou posterior: O `snapshot-policy` parâmetro é configurado automaticamente como nenhum durante a criação de armazenamento persistente.
  - ONTAP 9.14,1: O `snapshot-policy` parâmetro é configurado `none` durante a criação do volume.
- Torne o volume de armazenamento persistente inacessível para acesso de protocolo de usuário externo (CIFS/NFS) para evitar corrupção acidental ou exclusão dos Registros de eventos persistentes.
  - ONTAP 9.15,1 ou posterior: O ONTAP bloqueia automaticamente o volume do acesso de protocolo de usuário externo (CIFS/NFS) durante a criação do armazenamento persistente.
  - ONTAP 9.14,1: Depois de ativar o FPolicy, desmonte o volume no ONTAP para remover o caminho de junção. Isso o torna inacessível para acesso de protocolo de usuário externo (CIFS/NFS).

Para obter mais informações, "Armazenamentos persistentes de FPolicy"consulte e "Crie armazenamentos persistentes".

Failover de armazenamento persistente e giveback

O armazenamento persistente permanece como era quando o último evento foi recebido, quando há uma reinicialização inesperada ou FPolicy é desativado e ativado novamente. Após uma operação de takeover, novos eventos são armazenados e processados pelo nó do parceiro. Após uma operação de giveback, o armazenamento persistente retoma o processamento de quaisquer eventos não processados que possam permanecer de quando a aquisição do nó ocorreu. Os eventos ao vivo teriam prioridade sobre eventos não processados.

Se o volume de armazenamento persistente passar de um nó para outro no mesmo SVM, as notificações que ainda não foram processadas também serão movidas para o novo nó. Você precisa executar novamente `fpolicy persistent-store create` o comando em qualquer nó após o volume ser movido para garantir que as notificações pendentes sejam entregues ao servidor externo.

Configuração da política

A configuração do mecanismo externo FPolicy, eventos e escopo para SVMs pode melhorar sua experiência e segurança geral.

- Configuração do mecanismo externo FPolicy para SVMs:
  - Fornecer segurança adicional vem com um custo de desempenho. Ativar a comunicação SSL (Secure Sockets Layer) tem um efeito de desempenho no acesso a compartilhamentos.
  - O mecanismo externo FPolicy deve ser configurado com mais de um servidor FPolicy para fornecer resiliência e alta disponibilidade de processamento de notificações do servidor FPolicy.
- Configuração de eventos FPolicy para SVMs:

  O monitoramento das operações de arquivos influencia sua experiência geral. Por exemplo, filtrar as operações de arquivos indesejados no lado do armazenamento melhora sua experiência. A NetApp recomenda configurar a seguinte configuração:

  - Monitorar os tipos mínimos de operações de arquivos e permitir o número máximo de filtros sem quebrar o caso de uso.
  - Usando filtros para operações getattr, ler, escrever, abrir e fechar. Os ambientes de diretório base SMB e NFS têm uma alta porcentagem dessas operações.
- Configuração do escopo de FPolicy para SVMs:

  Restrinja o escopo das políticas aos objetos de storage relevantes, como compartilhamentos, volumes e exportações, em vez de habilitá-los em todo o SVM. O NetApp recomenda verificar as extensões do diretório. Se o `is-file-extension-check-on-directories-enabled` parâmetro estiver definido como `true`, os objetos de diretório serão submetidos às mesmas verificações de extensão que os arquivos normais.

Configuração de rede

A conetividade de rede entre o servidor FPolicy e o controlador deve ser de baixa latência. A NetApp recomenda separar o tráfego FPolicy do tráfego do cliente usando uma rede privada.

Além disso, você deve colocar servidores FPolicy externos (servidores FPolicy) próximo ao cluster com conetividade de alta largura de banda para fornecer latência mínima e conetividade de alta largura de banda.

Para um cenário em que o LIF para tráfego FPolicy é configurado em uma porta diferente para o LIF para tráfego de cliente, o FPolicy LIF pode falhar para o outro nó devido a uma falha de porta. Como resultado, o servidor FPolicy torna-se inacessível a partir do nó, o que faz com que as notificações FPolicy para operações de arquivo no nó falhem. Para evitar esse problema, verifique se o servidor FPolicy pode ser acessado por pelo menos um LIF no nó para processar solicitações FPolicy para as operações de arquivo executadas nesse nó.

Configuração de hardware

Você pode ter o servidor FPolicy em um servidor físico ou virtual. Se o servidor FPolicy estiver em um ambiente virtual, você deverá alocar recursos dedicados (CPU, rede e memória) ao servidor virtual.

A taxa de servidor nó para FPolicy do cluster deve ser otimizada para garantir que os servidores FPolicy não estejam sobrecarregados, o que pode introduzir latências quando o SVM responder às solicitações do cliente. A proporção ideal depende do aplicativo parceiro para o qual o servidor FPolicy está sendo usado. A NetApp recomenda trabalhar com parceiros para determinar o valor apropriado.

Configuração de várias políticas

A política de FPolicy para bloqueio nativo tem a prioridade mais alta, independentemente do número de sequência, e as políticas de alteração de decisões têm uma prioridade mais alta do que outras. A prioridade da política depende do caso de uso. A NetApp recomenda trabalhar com parceiros para determinar a prioridade apropriada.

Considerações de tamanho

O FPolicy executa monitoramento em linha de operações SMB e NFS, envia notificações para o servidor externo e aguarda uma resposta, dependendo do modo de comunicação do motor externo (síncrono ou assíncrono). Esse processo afeta o desempenho dos recursos de CPU e acesso SMB e NFS.

Para mitigar quaisquer problemas, a NetApp recomenda trabalhar com parceiros para avaliar e dimensionar o ambiente antes de habilitar o FPolicy. O desempenho é afetado por vários fatores, incluindo o número de usuários, caraterísticas da carga de trabalho, como operações por usuário e tamanho de dados, latência de rede e falha ou lentidão do servidor.

Monitorar o desempenho

FPolicy é um sistema baseado em notificações. As notificações são enviadas para um servidor externo para processamento e para gerar uma resposta de volta ao ONTAP. Esse processo de ida e volta aumenta a latência para o acesso do cliente.

O monitoramento dos contadores de desempenho no servidor FPolicy e no ONTAP oferece a capacidade de identificar gargalos na solução e ajustar os parâmetros conforme necessário para uma solução ideal. Por exemplo, um aumento na latência de FPolicy tem um efeito em cascata na latência de acesso SMB e NFS. Portanto, você deve monitorar a carga de trabalho (SMB e NFS) e a latência do FPolicy. Além disso, você pode usar políticas de qualidade do serviço no ONTAP para configurar um workload para cada volume ou SVM habilitado para FPolicy.

O NetApp recomenda executar o `statistics show –object workload` comando para exibir estatísticas de carga de trabalho. Além disso, você deve monitorar os seguintes parâmetros:

- Latências médias, de leitura e de gravação
- Número total de operações

- Contadores de leitura e escrita

Você pode monitorar o desempenho dos subsistemas FPolicy usando os seguintes contadores FPolicy.

Você deve estar no modo de diagnóstico para coletar estatísticas relacionadas ao FPolicy.

Passos

1. Recolher contadores FPolicy:
   a. `statistics start -object fpolicy -instance instance_name -sample-id ID`
   b. `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`
2. Visualizar contadores FPolicy:
   a. `statistics show -object fpolicy –instance instance_name -sample-id ID`
   b. `statistics show -object fpolicy_server –instance instance_name -sample-id ID`

   Os `fpolicy` contadores e `fpolicy_server` fornecem informações sobre vários parâmetros de desempenho descritos na tabela a seguir.

Contadores	Descrição
• contadores de "fpolicy"*	aborted_requests
Número de solicitações de tela para as quais o processamento é abortado no SVM	event_count
Lista de eventos que resultam em notificação	max_request_latency
Latência máxima de solicitações de tela	pedidos_pendentes
Número total de solicitações de tela em andamento	processed_requests
Número total de solicitações de tela que passaram pelo processamento de fpolicy no SVM	request_latency_hist
Histograma de latência para solicitações de tela	requests_despached_rate
Número de solicitações de tela enviadas por segundo	requests_received_rate

Contadores	Descrição
Número de solicitações de tela recebidas por segundo	• contadores de "fpolicy_server"*
max_request_latency	Latência máxima para uma solicitação de tela
pedidos_pendentes	Número total de solicitações de tela aguardando resposta
request_latency (latência_de	Latência média para solicitação de tela
request_latency_hist	Histograma de latência para solicitações de tela
request_sent_rate	Número de solicitações de tela enviadas ao servidor FPolicy por segundo
taxa de resposta_recebida	Número de respostas de tela recebidas do servidor FPolicy por segundo

Gerencie o fluxo de trabalho FPolicy e a dependência de outras tecnologias

A NetApp recomenda desativar uma política de FPolicy antes de fazer quaisquer alterações de configuração. Por exemplo, se você quiser adicionar ou modificar um endereço IP no mecanismo externo configurado para a política ativada, desative primeiro a política.

Se você configurar o FPolicy para monitorar volumes do NetApp FlexCache, o NetApp recomenda que você não configure o FPolicy para monitorar as operações de arquivos de leitura e getattr. O monitoramento dessas operações no ONTAP requer a recuperação de dados inode-to-path (I2P). Como os dados I2P não podem ser recuperados de volumes FlexCache, eles devem ser recuperados do volume de origem. Portanto, o monitoramento dessas operações elimina os benefícios de desempenho que o FlexCache pode oferecer.

Quando o FPolicy e uma solução antivírus off-box são implantados, a solução antivírus recebe notificações primeiro. O processamento de FPolicy é iniciado somente após a verificação antivírus estar concluída. É importante que você dimensione as soluções antivírus corretamente porque um scanner antivírus lento pode afetar o desempenho geral.

Considerações de atualização e reversão de passagem-leitura

Há certas considerações de atualização e reversão que você deve saber antes de atualizar para uma versão do ONTAP que suporta passagem-leitura ou antes de reverter para uma versão que não suporta passagem-leitura.

A atualizar

Depois que todos os nós são atualizados para uma versão do ONTAP que suporte a passagem-leitura FPolicy, o cluster é capaz de usar a funcionalidade de leitura de passagem; no entanto, a leitura de passagem é desativada por padrão nas configurações FPolicy existentes. Para usar a leitura de passagem em configurações FPolicy existentes, você deve desativar a política FPolicy e modificar a configuração e, em seguida, reativar a configuração.

Reverter

Antes de reverter para uma versão do ONTAP que não suporte a passagem-leitura de FPolicy, você deve atender às seguintes condições:

- Desative todas as políticas usando passthrough-read e, em seguida, modifique as configurações afetadas para que elas não usem passthrough-read.
- Desative a funcionalidade FPolicy no cluster desativando todas as políticas FPolicy no cluster.

Antes de reverter para uma versão do ONTAP que não ofereça suporte a armazenamentos persistentes, certifique-se de que nenhuma das diretivas FPolicy tenha um armazenamento persistente configurado. Se um armazenamento persistente estiver configurado, a reversão falhará.

Quais são os passos para configurar uma configuração FPolicy

Antes que o FPolicy possa monitorar o acesso a arquivos, uma configuração FPolicy deve ser criada e ativada na máquina virtual de storage (SVM) para a qual os serviços FPolicy são necessários.

As etapas para configurar e habilitar uma configuração FPolicy no SVM são as seguintes:

1. Crie um mecanismo externo FPolicy.

   O mecanismo externo FPolicy identifica os servidores FPolicy externos (servidores FPolicy) que estão associados a uma configuração FPolicy específica. Se o mecanismo FPolicy "'nativo" interno for usado para criar uma configuração nativa de bloqueio de arquivos, você não precisará criar um mecanismo externo FPolicy.

   Começando com ONTAP 9.15,1, você pode usar o `protobuf` formato do motor. Quando definido como `protobuf`, as mensagens de notificação são codificadas de forma binária usando o Google Protobuf. Antes de definir o formato do mecanismo como `protobuf`, certifique-se de que o servidor FPolicy também suporta `protobuf` a desserialização. Para obter mais informações, consulte "Planeie a configuração do motor externo FPolicy"

2. Criar um evento FPolicy.

   Um evento FPolicy descreve o que a política FPolicy deve monitorar. Os eventos consistem em protocolos e operações de arquivo a serem monitoradas e podem conter uma lista de filtros. Eventos Use filtros para restringir a lista de eventos monitorados para os quais o mecanismo externo FPolicy deve enviar notificações. Os eventos também especificam se a diretiva monitora as operações de volume.

3. Crie um armazenamento persistente FPolicy (opcional).

   A partir do ONTAP 9.14,1, o FPolicy permite que você configure "armazenamentos persistentes"para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

   Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente.

   A partir do ONTAP 9.15,1, a configuração de armazenamento persistente do FPolicy é simplificada. O `persistent-store-create` comando automatiza a criação de volume para o SVM e configura o volume para o armazenamento persistente.

4. Crie uma política FPolicy.

   A política FPolicy é responsável por associar, com o escopo apropriado, o conjunto de eventos que precisam ser monitorados e para qual das notificações de eventos monitorados deve ser enviado para o servidor FPolicy designado (ou para o mecanismo nativo se nenhum servidor FPolicy estiver configurado).

A política também define se o servidor FPolicy tem acesso privilegiado aos dados para os quais recebe notificações. Um servidor FPolicy precisa de acesso privilegiado se o servidor precisar acessar os dados. Os casos de uso típicos em que o acesso privilegiado é necessário incluem bloqueio de arquivos, gerenciamento de cotas e gerenciamento de storage hierárquico. A política é onde você especifica se a configuração para essa política usa um servidor FPolicy ou o servidor FPolicy interno "'nativo".

Uma política especifica se a triagem é obrigatória. Se a triagem for obrigatória e todos os servidores FPolicy estiverem inativos ou se nenhuma resposta for recebida dos servidores FPolicy dentro de um período de tempo limite definido, o acesso ao arquivo será negado.

Os limites de uma política são o SVM. Uma política não pode se aplicar a mais de um SVM. No entanto, um SVM específico pode ter várias políticas de FPolicy, cada uma com a mesma combinação ou diferente de configurações de escopo, evento e servidor externo.

5. Configure o escopo da política.

   O escopo da FPolicy determina quais volumes, compartilhamentos ou políticas de exportação a política atua ou exclui do monitoramento. Um escopo também determina quais extensões de arquivo devem ser incluídas ou excluídas do monitoramento FPolicy.

   Excluir listas têm precedência sobre incluir listas.

6. Ative a política FPolicy.

   Quando a política está ativada, os canais de controle e, opcionalmente, os canais de dados privilegiados são conetados. O processo de FPolicy nos nós nos quais o SVM participa começa a monitorar o acesso a arquivos e pastas e, para eventos que correspondam aos critérios configurados, envia notificações para os servidores FPolicy (ou para o mecanismo nativo se nenhum servidor FPolicy estiver configurado).

Se a política usar bloqueio de arquivos nativo, um mecanismo externo não será configurado ou associado à política.

Planeie a configuração do motor externo FPolicy

Planeie a configuração do motor externo FPolicy

Antes de configurar o mecanismo externo FPolicy, você deve entender o que significa criar um mecanismo externo e quais parâmetros de configuração estão disponíveis. Essas informações ajudam você a determinar quais valores definir para cada parâmetro.

Informações que são definidas ao criar o mecanismo externo FPolicy

A configuração do mecanismo externo define as informações que o FPolicy precisa para fazer e gerenciar conexões com os servidores FPolicy externos, incluindo o seguinte:

- Nome do SVM
- Nome do motor
- Os endereços IP dos servidores FPolicy primário e secundário e o número da porta TCP a serem usados ao fazer a conexão com os servidores FPolicy
- Se o tipo de motor é assíncrono ou síncrono
- Se o formato do motor é `xml` ou `protobuf`

Começando com ONTAP 9.15,1, você pode usar o `protobuf` formato do motor. Quando definido como `protobuf`, as mensagens de notificação são codificadas de forma binária usando o Google Protobuf. Antes de definir o formato do mecanismo como `protobuf`, certifique-se de que o servidor FPolicy também suporta `protobuf` a desserialização.

Uma vez que o formato protobuf é suportado a partir de ONTAP 9.15,1, você deve considerar o formato externo do motor antes de reverter para uma versão anterior do ONTAP. Se você reverter para uma versão anterior do ONTAP 9.15,1, trabalhe com seu parceiro FPolicy para:

- Altere cada formato do motor de `protobuf` para `xml`
- Elimine os motores com um formato de motor de `protobuf`

- Como autenticar a conexão entre o nó e o servidor FPolicy

  Se você optar por configurar a autenticação SSL mútua, você também deve configurar parâmetros que fornecem informações de certificado SSL.

- Como gerir a ligação utilizando várias definições avançadas de privilégios

  Isso inclui parâmetros que definem coisas como valores de tempo limite, valores de repetição, valores de keep-alive, valores máximos de solicitação, valores de tamanho de buffer enviados e recebidos e valores de tempo limite da sessão.

O `vserver fpolicy policy external-engine create` comando é usado para criar um mecanismo externo FPolicy.

Quais são os parâmetros básicos do motor externo

Você pode usar a seguinte tabela de parâmetros básicos de configuração do FPolicy para ajudá-lo a Planejar sua configuração:

Tipo de informação	Opção
SVM Especifica o nome do SVM que você deseja associar a esse mecanismo externo. Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.	`-vserver vserver_name`

Nome do motor Especifica o nome a ser atribuído à configuração externa do motor. Você deve especificar o nome do mecanismo externo mais tarde quando criar a política FPolicy. Isto associa o motor externo à política. O nome pode ter até 256 carateres. O nome deve ter até 200 carateres se estiver configurando o nome do mecanismo externo em uma configuração de recuperação de desastres do MetroCluster ou SVM. O nome pode conter qualquer combinação dos seguintes carateres de intervalo ASCII: • `a` através `z` • `A` através `Z` • `0` através `9` • "»_", "-", and "»."	`-engine-name engine_name`
Servidores FPolicy primários Especifica os servidores FPolicy primários para os quais o nó envia notificações para uma determinada política FPolicy. O valor é especificado como uma lista delimitada por vírgulas de endereços IP. Se mais de um endereço IP de servidor primário for especificado, cada nó no qual o SVM participa criará uma conexão de controle para cada servidor FPolicy primário especificado no momento em que a diretiva é ativada. Se você configurar vários servidores FPolicy primários, as notificações serão enviadas para os servidores FPolicy de forma redonda. Se o mecanismo externo for usado em uma configuração de recuperação de desastres do MetroCluster ou SVM, você deverá especificar os endereços IP dos servidores FPolicy no local de origem como servidores primários. Os endereços IP dos servidores FPolicy no local de destino devem ser especificados como servidores secundários.	`-primary-servers IP_address,...`
Número da porta Especifica o número da porta do serviço FPolicy.	`-port integer`

Servidores FPolicy secundários Especifica os servidores FPolicy secundários para os quais enviar eventos de acesso a arquivos para uma determinada política FPolicy. O valor é especificado como uma lista delimitada por vírgulas de endereços IP. Os servidores secundários são utilizados apenas quando nenhum dos servidores primários é alcançável. As conexões com servidores secundários são estabelecidas quando a diretiva está ativada, mas as notificações são enviadas para servidores secundários somente se nenhum dos servidores primários estiver acessível. Se você configurar vários servidores secundários, as notificações serão enviadas para os servidores FPolicy de forma redonda.	`-secondary-servers IP_address,...`
Tipo de motor externo Especifica se o mecanismo externo opera no modo síncrono ou assíncrono. Por padrão, o FPolicy opera no modo síncrono. Quando definido como `synchronous`, o processamento de solicitação de arquivo envia uma notificação para o servidor FPolicy, mas depois não continua até receber uma resposta do servidor FPolicy. Nesse ponto, o fluxo de solicitação continua ou o processamento resulta em negação, dependendo se a resposta do servidor FPolicy permite a ação solicitada. Quando definido como `asynchronous`, o processamento de solicitação de arquivo envia uma notificação para o servidor FPolicy e, em seguida, continua.	`-extern-engine-type external_engine_type` O valor para este parâmetro pode ser um dos seguintes: • `synchronous` • `asynchronous`
Formato externo do motor Especifique se o formato do mecanismo externo é xml ou protobuf. Começando com ONTAP 9.15,1, você pode usar o formato do mecanismo protobuf. Quando definido como protobuf, as mensagens de notificação são codificadas em forma binária usando o Google Protobuf. Antes de definir o formato do motor para protobuf, certifique-se de que o servidor FPolicy também suporta a desserialização de protobuf.	`- extern-engine-format` {`protobuf` ou `xml`

Opção SSL para comunicação com o servidor FPolicy Especifica a opção SSL para comunicação com o servidor FPolicy. Este é um parâmetro obrigatório. Você pode escolher uma das opções com base nas seguintes informações: • Quando definido como `no-auth`, não ocorre autenticação. O link de comunicação é estabelecido através do TCP. • Quando definido como `server-auth`, o SVM autentica o servidor FPolicy usando autenticação de servidor SSL. • Quando definido como `mutual-auth`, a autenticação mútua ocorre entre o SVM e o servidor FPolicy; o SVM autentica o servidor FPolicy e o servidor FPolicy autentica o SVM. Se você optar por configurar a autenticação SSL mútua, também deverá configurar os `-certificate-common-name` parâmetros , `-certificate-serial` e `-certifcate-ca` .	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`Selecione
Certificado FQDN ou nome comum personalizado Especifica o nome do certificado usado se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Você pode especificar o nome do certificado como um FQDN ou como um nome comum personalizado. Se você especificar `mutual-auth` para o `-ssl-option` parâmetro, será necessário especificar um valor para o `-certificate-common-name` parâmetro.	`-certificate-common -name` `text`
Número de série do certificado Especifica o número de série do certificado usado para autenticação se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Se você especificar `mutual-auth` para o `-ssl-option` parâmetro, será necessário especificar um valor para o `-certificate-serial` parâmetro.	`-certificate-serial` `text`
Autoridade de certificação Especifica o nome da CA do certificado usado para autenticação se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Se você especificar `mutual-auth` para o `-ssl-option` parâmetro, será necessário especificar um valor para o `-certificate-ca` parâmetro.	`-certificate-ca` `text`

Quais são as opções avançadas do motor externo

Você pode usar a seguinte tabela de parâmetros avançados de configuração FPolicy à medida que planeja personalizar sua configuração com parâmetros avançados. Você usa esses parâmetros para modificar o comportamento de comunicação entre os nós de cluster e os servidores FPolicy:

Tipo de informação	Opção
Tempo limite para cancelar uma solicitação Especifica o intervalo de tempo em horas (`h`), (`m`minutos) ou segundos (`s`) que o nó espera por uma resposta do servidor FPolicy. Se o intervalo de tempo limite passar, o nó envia uma solicitação de cancelamento para o servidor FPolicy. O nó então envia a notificação para um servidor FPolicy alternativo. Esse tempo limite ajuda a lidar com um servidor FPolicy que não está respondendo, o que pode melhorar a resposta do cliente SMB/NFS. Além disso, cancelar solicitações após um período de tempo limite pode ajudar a liberar recursos do sistema porque a solicitação de notificação é movida de um servidor FPolicy inativo/ruim para um servidor FPolicy alternativo. O intervalo para este valor é `0` através `100`de . Se o valor estiver definido como `0`, a opção será desativada e as mensagens de solicitação de cancelamento não serão enviadas para o servidor FPolicy. A predefinição é `20s`.	`-reqs-cancel-timeout integer`[h
m	s]
Tempo limite para abortar uma solicitação Especifica o tempo limite em horas (`h`), (`m`minutos) ou segundos (`s`) para abortar uma solicitação. O intervalo para este valor é `0` através `200`de .	`-reqs-abort-timeout ` `integer`[h
m	s]
Intervalo para envio de solicitações de status Especifica o intervalo em horas (`h`), minutos (`m`) ou segundos (`s`) após o qual uma solicitação de status é enviada ao servidor FPolicy. O intervalo para este valor é `0` através `50`de . Se o valor estiver definido como `0`, a opção será desativada e as mensagens de solicitação de status não serão enviadas ao servidor FPolicy. A predefinição é `10s`.	`-status-req-interval integer`[h
m	s]

Máximo de solicitações pendentes no servidor FPolicy Especifica o número máximo de solicitações pendentes que podem ser enfileiradas no servidor FPolicy. O intervalo para este valor é `1` através `10000`de . A predefinição é `500`.	`-max-server-reqs integer`
Tempo limite para desconetar um servidor FPolicy não responsivo Especifica o intervalo de tempo em horas (`h`), (`m`minutos) ou segundos (`s`) após o qual a conexão com o servidor FPolicy é encerrada. A conexão é encerrada após o período de tempo limite somente se a fila do servidor FPolicy contiver o máximo de solicitações permitidas e nenhuma resposta for recebida dentro do período de tempo limite. O número máximo permitido de solicitações é `50` (o padrão) ou o número especificado pelo `max-server-reqs-` parâmetro. O intervalo para este valor é `1` através `100`de . A predefinição é `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervalo para enviar mensagens keep-alive para o servidor FPolicy Especifica o intervalo de tempo em horas (`h`), (`m`minutos) ou segundos (`s`) no qual as mensagens keep-alive são enviadas ao servidor FPolicy. As mensagens keep-alive detetam conexões semi-abertas. O intervalo para este valor é `10` através `600`de . Se o valor estiver definido como `0`, a opção será desativada e as mensagens de manutenção em tempo real serão impedidas de serem enviadas para os servidores FPolicy. A predefinição é `120s`.	`-keep-alive-interval- integer`[h
m	s]
Máximo de tentativas de reconexão Especifica o número máximo de vezes que o SVM tenta se reconetar ao servidor FPolicy depois que a conexão foi interrompida. O intervalo para este valor é `0` através `20`de . A predefinição é `5`.	`-max-connection-retries integer`

Receive buffer size Especifica o tamanho do buffer de receção do soquete conetado para o servidor FPolicy. O valor padrão é definido como 256 kilobytes (Kb). Quando o valor é definido como 0, o tamanho do buffer de receção é definido para um valor definido pelo sistema. Por exemplo, se o tamanho padrão do buffer de recebimento do soquete for de 65536 bytes, definindo o valor ajustável como 0, o tamanho do buffer do soquete será definido como 65536 bytes. Você pode usar qualquer valor não padrão para definir o tamanho (em bytes) do buffer de recebimento.	`-recv-buffer-size integer`
Enviar tamanho do buffer Especifica o tamanho do buffer de envio do soquete conetado para o servidor FPolicy. O valor padrão é definido como 256 kilobytes (Kb). Quando o valor é definido como 0, o tamanho do buffer de envio é definido para um valor definido pelo sistema. Por exemplo, se o tamanho padrão do buffer de envio do soquete for definido como 65536 bytes, definindo o valor ajustável como 0, o tamanho do buffer do soquete será definido como 65536 bytes. Você pode usar qualquer valor não padrão para definir o tamanho (em bytes) do buffer de envio.	`-send-buffer-size integer`
Tempo limite para purgar um Session ID durante a reconexão Especifica o intervalo em horas (`h`), minutos (`m`) ou segundos (`s`) após o qual um novo Session ID é enviado ao servidor FPolicy durante tentativas de reconexão. Se a conexão entre o controlador de armazenamento e o servidor FPolicy for encerrada e a nova conexão for feita dentro do `-session-timeout` intervalo, o Session ID antigo será enviado para o servidor FPolicy para que ele possa enviar respostas para notificações antigas. O valor padrão é definido para 10 segundos.	`-session-timeout integer[ m][integers]`

Informações adicionais sobre a configuração de mecanismos externos FPolicy para usar conexões autenticadas SSL

Você precisa saber algumas informações adicionais se quiser configurar o mecanismo externo FPolicy para usar SSL ao se conetar a servidores FPolicy.

Autenticação de servidor SSL

Se você optar por configurar o mecanismo externo FPolicy para autenticação de servidor SSL, antes de criar o mecanismo externo, você deverá instalar o certificado público da autoridade de certificação (CA) que assinou o certificado do servidor FPolicy.

Autenticação mútua

Se você configurar mecanismos externos do FPolicy para usar a autenticação mútua SSL ao conetar LIFs de dados da máquina virtual de armazenamento (SVM) a servidores FPolicy externos, antes de criar o mecanismo externo, você deverá instalar o certificado público da CA que assinou o certificado do servidor FPolicy juntamente com o certificado público e o arquivo chave para autenticação do SVM. Você não deve excluir este certificado enquanto nenhuma política FPolicy estiver usando o certificado instalado.

Se o certificado for excluído enquanto o FPolicy estiver usando-o para autenticação mútua ao se conetar a um servidor FPolicy externo, não será possível reativar uma política FPolicy desativada que use esse certificado. A política FPolicy não pode ser reativada nessa situação mesmo que um novo certificado com as mesmas configurações seja criado e instalado no SVM.

Se o certificado tiver sido excluído, você precisará instalar um novo certificado, criar novos mecanismos externos FPolicy que usam o novo certificado e associar os novos mecanismos externos à política FPolicy que você deseja reativar modificando a política FPolicy.

Instale certificados para SSL

O certificado público da CA que é usado para assinar o certificado do servidor FPolicy é instalado usando o `security certificate install` comando com o `-type` parâmetro definido como `client-ca`. A chave privada e o certificado público necessários para a autenticação do SVM são instalados usando o `security certificate install` comando com o `-type` parâmetro definido como `server`.

Os certificados não são replicados nas relações de recuperação de desastres do SVM com uma configuração que não preserve ID

Os certificados de segurança usados para autenticação SSL ao fazer conexões com servidores FPolicy não são replicados para destinos de recuperação de desastres SVM com configurações que não preservem ID. Embora a configuração do mecanismo externo FPolicy na SVM seja replicada, os certificados de segurança não são replicados. Tem de instalar manualmente os certificados de segurança no destino.

Quando você configura a relação de recuperação de desastres SVM, o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), todos os detalhes de configuração do FPolicy serão replicados, incluindo as informações do certificado de segurança. Só tem de instalar os certificados de segurança no destino se definir a opção como `false` (non-ID-Preserve).

Restrições para mecanismos externos de FPolicy com escopo de cluster com configurações de recuperação de desastres MetroCluster e SVM

Você pode criar um mecanismo externo FPolicy com escopo de cluster atribuindo a máquina virtual de armazenamento de cluster (SVM) ao mecanismo externo. No entanto, ao criar um mecanismo externo com escopo de cluster em uma configuração de recuperação de desastres MetroCluster ou SVM, há certas restrições ao escolher o método de autenticação usado pelo SVM para comunicação externa com o servidor FPolicy.

Há três opções de autenticação que você pode escolher ao criar servidores FPolicy externos: sem autenticação, autenticação de servidor SSL e autenticação mútua SSL. Embora não haja restrições ao

escolher a opção de autenticação se o servidor FPolicy externo for atribuído a um SVM de dados, há restrições ao criar um mecanismo externo FPolicy com escopo de cluster:

Configuração	Permitido?
Recuperação de desastres MetroCluster ou SVM e um mecanismo externo FPolicy com escopo de cluster sem autenticação (SSL não está configurado)	Sim
Recuperação de desastres MetroCluster ou SVM e um mecanismo externo FPolicy com escopo de cluster com autenticação mútua SSL ou SSL	Não

- Se houver um mecanismo externo FPolicy com escopo de cluster e autenticação SSL e você quiser criar uma configuração de recuperação de desastres do MetroCluster ou SVM, modifique esse mecanismo externo para não usar autenticação ou remover o mecanismo externo antes de criar a configuração de recuperação de desastres do MetroCluster ou SVM.
- Se a configuração de recuperação de desastres do MetroCluster ou SVM já existir, o ONTAP impede que você crie um mecanismo externo FPolicy com escopo de cluster com autenticação SSL.

Preencha a folha de cálculo de configuração do motor externo FPolicy

Você pode usar esta Planilha para Registrar os valores que você precisa durante o processo de configuração do mecanismo externo FPolicy. Se um valor de parâmetro for necessário, você precisará determinar qual valor usar para esses parâmetros antes de configurar o mecanismo externo.

Informações para uma configuração externa básica do motor

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do mecanismo externo e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome do motor	Sim	Sim	
Servidores FPolicy primários	Sim	Sim	
Número da porta	Sim	Sim	
Servidores FPolicy secundários	Não		
Tipo de motor externo	Não		
Opção SSL para comunicação com servidor FPolicy externo	Sim	Sim	

Certificado FQDN ou nome comum personalizado	Não		
Número de série do certificado	Não		
Autoridade de certificação	Não		

Informações para parâmetros externos avançados do motor

Para configurar um motor externo com parâmetros avançados, tem de introduzir o comando de configuração no modo de privilégio avançado.

Tipo de informação	Obrigatório	Incluir	Seus valores
Tempo limite para cancelar uma solicitação	Não		
Tempo limite para abortar uma solicitação	Não		
Intervalo para envio de solicitações de status	Não		
Máximo de solicitações pendentes no servidor FPolicy	Não		
Tempo limite para desconetar um servidor FPolicy não responsivo	Não		
Intervalo para enviar mensagens keep-alive para o servidor FPolicy	Não		
Máximo de tentativas de reconexão	Não		
Receber tamanho do buffer	Não		
Enviar tamanho do buffer	Não		
Tempo limite para purgar um Session ID durante a reconexão	Não		

Planeje a configuração do evento FPolicy

Planeje a visão geral da configuração de eventos FPolicy

Antes de configurar eventos FPolicy, você deve entender o que significa criar um evento FPolicy. Você deve determinar quais protocolos deseja que o evento monitore, quais eventos monitorar e quais filtros de eventos usar. Essas informações ajudam a Planejar

os valores que você deseja definir.

O que significa criar um evento FPolicy

Criar o evento FPolicy significa definir as informações que o processo FPolicy precisa para determinar quais operações de acesso a arquivos monitorar e para quais notificações de eventos monitorados devem ser enviadas para o servidor FPolicy externo. A configuração do evento FPolicy define as seguintes informações de configuração:

- Nome da máquina virtual de storage (SVM)
- Nome do evento
- Quais protocolos monitorar

  O FPolicy pode monitorar SMB, NFSv3, NFSv4 e, a partir de operações de acesso a arquivos ONTAP 9.15,1, NFSv4,1.

- Quais operações de arquivo monitorar

  Nem todas as operações de arquivo são válidas para cada protocolo.

- Quais filtros de arquivo configurar

  Apenas determinadas combinações de operações de arquivo e filtros são válidas. Cada protocolo tem seu próprio conjunto de combinações suportadas.

- Se deve monitorar a montagem de volume e desmontar operações

> Existe uma dependência com três dos parâmetros (`-protocol`, `-file-operations`, `-filters`). As seguintes combinações são válidas para os três parâmetros:
>
> - Pode especificar os `-protocol` parâmetros e. `-file-operations`
> - Você pode especificar todos os três parâmetros.
> - Não é possível especificar nenhum dos parâmetros.

O que contém a configuração do evento FPolicy

Você pode usar a seguinte lista de parâmetros de configuração de eventos FPolicy disponíveis para ajudá-lo a Planejar sua configuração:

Tipo de informação	Opção
SVM Especifica o nome do SVM que você deseja associar a este evento FPolicy. Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.	`-vserver vserver_name`

Nome do evento Especifica o nome a ser atribuído ao evento FPolicy. Quando você cria a política FPolicy, você associa o evento FPolicy à política usando o nome do evento. O nome pode ter até 256 carateres. O nome deve ter até 200 carateres se o evento for configurado em uma configuração de recuperação de desastres do MetroCluster ou SVM. O nome pode conter qualquer combinação dos seguintes carateres de intervalo ASCII: • `a` através `z` • `A` através `Z` • `0` através `9` • "`_`,"`-`", `and` ".».	`-event-name event_name`
Protocolo Especifica qual protocolo configurar para o evento FPolicy. A lista para `-protocol` pode incluir um dos seguintes valores: • `cifs` • `nfsv3` • `nfsv4` Se você especificar `-protocol`, então você deve especificar um valor válido no `-file-operations` parâmetro. À medida que a versão do protocolo muda, os valores válidos podem mudar. A partir do ONTAP 9.15,1, o NFSv4 permite capturar eventos NFSv4,0 e NFSv4,1.	`-protocol protocol`

Operações de arquivo Especifica a lista de operações de arquivo para o evento FPolicy. O evento verifica as operações especificadas nesta lista a partir de todas as solicitações de cliente usando o protocolo especificado no `-protocol` parâmetro. Você pode listar uma ou mais operações de arquivo usando uma lista delimitada por vírgulas. A lista para `-file-operations` pode incluir um ou mais dos seguintes valores: • `close` para operações de fechamento de arquivo • `create` para operações de criação de arquivo • `create-dir` para operações de criação de diretório • `delete` para operações de exclusão de arquivos • `delete_dir` para operações de exclusão de diretório • `getattr` para obter operações de atributo • `link` para operações de link • `lookup` para operações de pesquisa • `open` para operações de arquivo aberto • `read` para operações de leitura de arquivos • `write` para operações de gravação de arquivos • `rename` para operações de renomeação de arquivo • `rename_dir` para operações de renomeação de diretório • `setattr` para definir operações de atributo • `symlink` para operações de link simbólico Se especificar `-file-operations`, deve especificar um protocolo válido no `-protocol` parâmetro.	`-file-operations file_operations,...`

Filtros Especifica a lista de filtros para uma determinada operação de arquivo para o protocolo especificado. Os valores no `-filters` parâmetro são usados para filtrar as solicitações do cliente. A lista pode incluir um ou mais dos seguintes itens: Se você especificar o `-filters` parâmetro, também deverá especificar valores válidos para os `-file-operations` parâmetros e. `-protocol` • `monitor-ads` opção para filtrar a solicitação do cliente para fluxo de dados alternativo. • `close-with-modification` opção para filtrar a solicitação do cliente para fechar com modificação. • `close-without-modification` opção para filtrar a solicitação do cliente para fechar sem modificação. • `first-read` opção para filtrar a solicitação do cliente para primeira leitura. • `first-write` opção para filtrar a solicitação do cliente para a primeira gravação. • `offline-bit` opção para filtrar a solicitação do cliente para o conjunto de bits off-line. A configuração desse filtro resulta no servidor FPolicy recebendo notificações somente quando os arquivos off-line são acessados. • `open-with-delete-intent` opção para filtrar a solicitação do cliente para abrir com delete intent. A configuração desse filtro faz com que o servidor FPolicy receba notificações somente quando for feita uma tentativa de abrir um arquivo com a intenção de excluí-lo. Isso é usado por sistemas de arquivos quando o `FILE_DELETE_ON_CLOSE` sinalizador é especificado. • `open-with-write-intent` opção para filtrar a solicitação do cliente para aberta com intenção de gravação. A configuração desse filtro faz com que o servidor FPolicy receba notificações somente quando for feita uma tentativa de abrir um arquivo com a intenção de escrever algo nele. • `write-with-size-change` opção para filtrar a solicitação do cliente para gravação com alteração de tamanho. • `setattr-with-owner-change` opção para filtrar as solicitações de setattr do cliente para alterar o proprietário de um arquivo ou de um diretório. • `setattr-with-group-change` opção para filtrar as solicitações de setattr do cliente para alterar o grupo de um arquivo ou um diretório. `setattr-with-sacl-change` Opção para filtrar as solicitações de setattr do cliente para alterar o SACL em um arquivo ou diretório. Este filtro está disponível apenas para os protocolos SMB e NFSv4.	`-filters filter, ...`

É a operação de volume necessária Especifica se o monitoramento é necessário para operações de montagem de volume e desmontagem. A predefinição é `false`.	`-volume-operation {true`
`false`Selecione `-filters filter, ...	*FPolicy Acesso negado notificações* A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. Essas notificações são valiosas para segurança, proteção contra ransomware e governança. As notificações serão geradas para a operação do arquivo falhou devido à falta de permissão, o que inclui: • Falhas devido a permissões NTFS. • Falhas devido a bits de modo Unix. • Falhas devido a ACLs NFSv4.
`-monitor-fileop-failure {true	`false`Selecione

Quando esse filtro é especificado, as operações de diretório não são monitoradas.

Operação de arquivo suportada e combinações de filtro que o FPolicy pode monitorar para SMB

Ao configurar seu evento FPolicy, você precisa estar ciente de que apenas determinadas combinações de operações de arquivo e filtros são suportadas para monitorar operações de acesso a arquivos SMB.

A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos SMB é fornecida na tabela a seguir:

Operações de arquivos compatíveis	Filtros suportados
fechar	monitor-ads, off-line-bit, close-com-modificação, close-sem-modificação, close-com-leitura, exclude-diretório
criar	monitor-anúncios, off-line-bit
criar_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.

eliminar	monitor-anúncios, off-line-bit
delete_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
getattr	offline-bit, exclude-dir
abrir	monitore anúncios, off-line-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
leia	monitore anúncios, off-line-bit, primeira leitura
escreva	monitore anúncios, off-line-bit, primeira gravação, write-with-size-change
mudar o nome	monitor-anúncios, off-line-bit
rename_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
ajuste	monitor-ads, off-line-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_time_change

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. A lista de combinações de filtro e operação de arquivo negado de acesso com suporte para monitoramento FPolicy de eventos de acesso a arquivos SMB é fornecida na tabela a seguir:

Acesso suportado operação de arquivo negado	Filtros suportados
abrir	NA

Operação de arquivo suportada e combinações de filtro que o FPolicy pode monitorar para NFSv3

Ao configurar seu evento FPolicy, você precisa estar ciente de que apenas certas combinações de operações de arquivo e filtros são suportadas para monitorar operações de acesso a arquivos NFSv3.

A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 é fornecida na seguinte tabela:

Operações de arquivos compatíveis	Filtros suportados
criar	bit offline
criar_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.

eliminar	bit offline
delete_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
link	bit offline
pesquisa	offline-bit, exclude-dir
leia	offline-bit, primeira leitura
escreva	offline-bit, primeira gravação, write-with-size-change
mudar o nome	bit offline
rename_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
ajuste	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
link simbólico	bit offline

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. A lista de combinações de filtro e operação de arquivo negado de acesso suportado para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 é fornecida na seguinte tabela:

Acesso suportado operação de arquivo negado	Filtros suportados
acesso	NA
criar	NA
criar_dir	NA
eliminar	NA
delete_dir	NA
link	NA
leia	NA
mudar o nome	NA

rename_dir	NA
ajuste	NA
escreva	NA

Operação de arquivo suportada e combinações de filtro que o FPolicy pode monitorar para NFSv4

Ao configurar seu evento FPolicy, você precisa estar ciente de que apenas certas combinações de operações de arquivo e filtros são suportadas para monitorar operações de acesso a arquivos NFSv4.

A partir do ONTAP 9.15,1, o FPolicy suporta o protocolo NFSv4,1.

A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv4 ou NFSv4,1 é fornecida na seguinte tabela:

Operações de arquivos compatíveis	Filtros suportados
fechar	offline-bit, exclude-directory
criar	bit offline
criar_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
eliminar	bit offline
delete_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.
getattr	offline-bit, exclude-directory
link	bit offline
pesquisa	offline-bit, exclude-directory
abrir	offline-bit, exclude-directory
leia	offline-bit, primeira leitura
escreva	offline-bit, primeira gravação, write-with-size-change
mudar o nome	bit offline
rename_dir	Atualmente, nenhum filtro é suportado para esta operação de arquivo.

ajuste	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_time_change, setattr_change, setattr_time_change, setattr_change
link simbólico	bit offline

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. A lista de combinações de filtro e operação de arquivo negado de acesso com suporte para monitoramento FPolicy de eventos de acesso a arquivos NFSv4 ou NFSv4,1 é fornecida na tabela a seguir:

Acesso suportado operação de arquivo negado	Filtros suportados
acesso	NA
criar	NA
criar_dir	NA
eliminar	NA
delete_dir	NA
link	NA
abrir	NA
leia	NA
mudar o nome	NA
rename_dir	NA
ajuste	NA
escreva	NA

Preencha a Planilha de configuração de evento FPolicy

Você pode usar essa Planilha para Registrar os valores necessários durante o processo de configuração de evento FPolicy. Se um valor de parâmetro for necessário, você precisará determinar qual valor usar para esses parâmetros antes de configurar o evento FPolicy.

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do evento FPolicy e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome do evento	Sim	Sim	
Protocolo	Não		
Operações de arquivos	Não		
Filtros	Não		
Operação de volume	Não		
Acesse eventos negados (suporte a partir de ONTAP 9.13)	Não		

Planeie a configuração da política FPolicy

Planeje a visão geral da configuração da política FPolicy

Antes de configurar a política FPolicy, você deve entender quais parâmetros são necessários ao criar a política, bem como por que você pode querer configurar determinados parâmetros opcionais. Essas informações ajudam você a determinar quais valores definir para cada parâmetro.

Ao criar uma política FPolicy, você associa a política ao seguinte:

- A máquina virtual de storage (SVM)
- Um ou mais eventos FPolicy
- Um motor externo FPolicy

Você também pode configurar várias configurações de política opcionais.

O que contém a configuração da política FPolicy

Você pode usar a seguinte lista de parâmetros opcionais e de política FPolicy disponíveis para ajudá-lo a Planejar sua configuração:

Tipo de informação	Opção	Obrigatório	Padrão
Nome da SVM Especifica o nome do SVM no qual você deseja criar uma política de FPolicy.	`-vserver vserver_name`	Sim	Nenhum

Nome da política Especifica o nome da política FPolicy. O nome pode ter até 256 carateres. O nome deve ter até 200 carateres se a diretiva estiver configurada em uma configuração de recuperação de desastres do MetroCluster ou SVM. O nome pode conter qualquer combinação dos seguintes carateres de intervalo ASCII: • `a` através `z` • `A` através `Z` • `0` através `9` • "»_", "`-`", `and` "»."	`-policy-name policy_name`	Sim	Nenhum
Nomes de eventos Especifica uma lista delimitada por vírgulas de eventos a serem associados à política FPolicy. • Você pode associar mais de um evento a uma política. • Um evento é específico de um protocolo. • Você pode usar uma única política para monitorar eventos de acesso a arquivos para mais de um protocolo, criando um evento para cada protocolo que você deseja que a diretiva monitore e associando os eventos à política. • Os eventos já devem existir.	`-events event_name, ...`	Sim	Nenhum
Armazenamento persistente A partir do ONTAP 9.14,1, este parâmetro especifica o armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM.	`-persistent -store persistent_store_name`	Não	Nenhum

Nome externo do motor Especifica o nome do mecanismo externo a ser associado à política FPolicy. • Um mecanismo externo contém informações exigidas pelo nó para enviar notificações para um servidor FPolicy. • Você pode configurar o FPolicy para usar o mecanismo externo nativo do ONTAP para bloqueio de arquivos simples ou para usar um mecanismo externo configurado para usar servidores FPolicy externos (servidores FPolicy) para bloqueio de arquivos e gerenciamento de arquivos mais sofisticados. • Se você quiser usar o mecanismo externo nativo, você não pode especificar um valor para esse parâmetro ou pode especificar `native` como o valor. • Se você quiser usar servidores FPolicy, a configuração para o mecanismo externo já deve existir.	`-engine engine_name`	Sim (a menos que a política use o mecanismo nativo do ONTAP interno)	`native`
É obrigatório rastreio Especifica se a triagem obrigatória de acesso a arquivos é necessária. • A configuração de triagem obrigatória determina qual ação é tomada em um evento de acesso a arquivos em um caso em que todos os servidores primário e secundário estão inativos ou nenhuma resposta é recebida dos servidores FPolicy dentro de um determinado período de tempo limite. • Quando definido como `true`, os eventos de acesso ao arquivo são negados. • Quando definido como `false`, eventos de acesso a arquivos são permitidos.	`-is-mandatory {true`	`false`Selecione	Não

`true`	*Permitir acesso privilegiado* Especifica se você deseja que o servidor FPolicy tenha acesso privilegiado aos arquivos e pastas monitorados usando uma conexão de dados privilegiada. Se configurado, os servidores FPolicy podem acessar arquivos da raiz do SVM que contém os dados monitorados usando a conexão de dados privilegiada. Para acesso privilegiado a dados, o SMB deve ser licenciado no cluster e todas as LIFs de dados usadas para se conetar aos servidores FPolicy devem ser configuradas para ter `cifs` como um dos protocolos permitidos. Se você quiser configurar a diretiva para permitir acesso privilegiado, você também deve especificar o nome de usuário para a conta que deseja que o servidor FPolicy use para acesso privilegiado.	`-allow -privileged -access {yes`	`no`Selecione

Não (a menos que a leitura de passagem esteja ativada)	`no`	*Nome de usuário privilegiado* Especifica o nome de usuário da conta que os servidores FPolicy usam para acesso privilegiado a dados. • O valor para este parâmetro deve usar o formato "nome de usuário". • Se `-allow -privileged -access` estiver definido como `no`, qualquer valor definido para este parâmetro será ignorado.	`-privileged -user-name user_name`

Não (a menos que o acesso privilegiado esteja ativado)	Nenhum	*Permitir passagem-leitura* Especifica se os servidores FPolicy podem fornecer serviços de leitura de passagem para arquivos que foram arquivados em armazenamento secundário (arquivos off-line) pelos servidores FPolicy: • A passagem-leitura é uma maneira de ler dados para arquivos off-line sem restaurar os dados para o armazenamento primário. A passagem-leitura reduz as latências de resposta porque não há necessidade de recuperar arquivos de volta ao storage primário antes de responder à solicitação de leitura. Além disso, a passagem-leitura otimiza a eficiência de storage eliminando a necessidade de consumir espaço de storage primário com arquivos que são recuperados exclusivamente para atender às solicitações de leitura. Quando ativado,	`-is-passthrough -read-enabled {true`

Requisito para configurações de escopo FPolicy se a política FPolicy usar o mecanismo nativo

Se você configurar a política FPolicy para usar o mecanismo nativo, há um requisito específico para como definir o escopo FPolicy configurado para a política.

O escopo FPolicy define os limites nos quais a política FPolicy se aplica, por exemplo, se a FPolicy se aplica a volumes ou compartilhamentos especificados. Existem vários parâmetros que restringem ainda mais o escopo ao qual a política FPolicy se aplica. Um desses parâmetros, `-is-file-extension-check-on-directories-enabled`, especifica se deve verificar as extensões de arquivo nos diretórios. O valor padrão é `false`, o que significa que as extensões de arquivo nos diretórios não estão marcadas.

Quando uma diretiva FPolicy que usa o mecanismo nativo está ativada em um compartilhamento ou volume e o `-is-file-extension-check-on-directories-enabled` parâmetro é definido como `false` para o escopo da política, o acesso ao diretório é negado. Com essa configuração, como as extensões de arquivo não são verificadas para diretórios, qualquer operação de diretório é negada se ela estiver sob o escopo da política.

Para garantir que o acesso ao diretório seja bem-sucedido ao usar o mecanismo nativo, você deve definir o `-is-file-extension-check-on-directories-enabled parameter` para `true` ao criar o escopo.

Com este parâmetro definido como `true`, as verificações de extensão acontecem para operações de diretório e a decisão de permitir ou negar acesso é tomada com base nas extensões incluídas ou excluídas na configuração do escopo FPolicy.

- os servidores FPolicy fornecem os dados para o arquivo em um canal de dados privilegiado separado aberto especificamente para leituras de passagem.
- Se você quiser configurar a passagem-leitura, a política também deve ser configurada para permitir acesso privilegiado.

Preencha a Planilha de política FPolicy

Você pode usar essa Planilha para Registrar os valores necessários durante o processo de configuração da política FPolicy. Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração da política FPolicy e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	
Nome da política	Sim	
Nomes de eventos	Sim	
Armazenamento persistente		
Nome do motor externo		
É necessário um rastreio obrigatório?		
Permitir acesso privilegiado		
Nome de usuário privilegiado		

A leitura de passagem está ativada?		

Planeje a configuração do escopo do FPolicy

Planeje a visão geral da configuração do escopo da FPolicy

Antes de configurar o escopo FPolicy, você deve entender o que significa criar um escopo. Você deve entender o que a configuração do escopo contém. Você também precisa entender quais são as regras de escopo de precedência. Essas informações podem ajudá-lo a Planejar os valores que você deseja definir.

O que significa criar um escopo FPolicy

Criar o escopo FPolicy significa definir os limites nos quais a política FPolicy se aplica. A máquina virtual de storage (SVM) é o limite básico. Ao criar um escopo para uma política de FPolicy, você deve definir a política de FPolicy à qual será aplicada e designar a qual SVM você deseja aplicar o escopo.

Há vários parâmetros que restringem ainda mais o escopo dentro do SVM especificado. Você pode restringir o escopo especificando o que incluir no escopo ou especificando o que excluir do escopo. Depois de aplicar um escopo a uma política habilitada, as verificações de eventos de política são aplicadas ao escopo definido por este comando.

As notificações são geradas para eventos de acesso a arquivos onde as correspondências são encontradas nas opções "'include'". As notificações não são geradas para eventos de acesso a arquivos em que as correspondências são encontradas nas opções "'excluir'".

A configuração do escopo da FPolicy define as seguintes informações de configuração:

- Nome do SVM
- Nome da política
- As ações a incluir ou excluir do que é monitorado
- As políticas de exportação para incluir ou excluir do que é monitorado
- Os volumes a incluir ou excluir do que é monitorado
- As extensões de arquivo para incluir ou excluir do que é monitorado
- Se a extensão de arquivo deve ser feita verifica em objetos de diretório

> Existem considerações especiais para o escopo de uma política de FPolicy de cluster. A política de FPolicy de cluster é uma política que o administrador do cluster cria para o SVM admin. Se o administrador do cluster também criar o escopo dessa política de FPolicy do cluster, o administrador SVM não poderá criar um escopo para essa mesma política. No entanto, se o administrador do cluster não criar um escopo para a política de FPolicy do cluster, qualquer administrador SVM poderá criar o escopo dessa política de cluster. Se o administrador do SVM criar um escopo para essa política de FPolicy de cluster, o administrador do cluster não poderá criar posteriormente um escopo de cluster para essa mesma política de cluster. Isso ocorre porque o administrador do cluster não pode substituir o escopo da mesma diretiva de cluster.

Quais são as regras de escopo de precedência

As seguintes regras de precedência se aplicam às configurações do escopo:

- Quando um compartilhamento é incluído no `-shares-to-include` parâmetro e o volume pai do compartilhamento é incluído no `-volumes-to-exclude` parâmetro, `-volumes-to-exclude` tem precedência sobre `-shares-to-include`.
- Quando uma política de exportação é incluída no `-export-policies-to-include` parâmetro e o volume pai da política de exportação é incluído no `-volumes-to-exclude` parâmetro, `-volumes-to-exclude` tem precedência sobre `-export-policies-to-include`.
- Um administrador pode especificar as `-file-extensions-to-include` listas e `-file-extensions-to-exclude` .

  O `-file-extensions-to-exclude` parâmetro é verificado antes de o `-file-extensions-to-include` parâmetro ser verificado.

O que contém a configuração do escopo do FPolicy

Você pode usar a seguinte lista de parâmetros de configuração do escopo FPolicy disponíveis para ajudá-lo a Planejar sua configuração:

> Ao configurar quais compartilhamentos, políticas de exportação, volumes e extensões de arquivo para incluir ou excluir do escopo, os parâmetros incluir e excluir podem incluir metacaracters como ""?" `and` "*". O uso de expressões regulares não é suportado.

Tipo de informação	Opção
SVM Especifica o nome do SVM no qual você deseja criar um escopo FPolicy. Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.	`-vserver vserver_name`
Nome da política Especifica o nome da política FPolicy à qual você deseja anexar o escopo. A política FPolicy já deve existir.	`-policy-name policy_name`
Compartilhamentos para incluir Especifica uma lista delimitada por vírgulas de compartilhamentos para monitorar a política FPolicy à qual o escopo é aplicado.	`-shares-to-include share_name, ...`

Compartilhamentos para excluir Especifica uma lista delimitada por vírgulas de compartilhamentos a serem excluídos do monitoramento para a política FPolicy à qual o escopo é aplicado.	`-shares-to-exclude share_name, ...`
Volumes a incluir especifica uma lista delimitada por vírgulas de volumes a monitorar para a política FPolicy à qual o escopo é aplicado.	`-volumes-to-include volume_name, ...`
Volumes a excluir Especifica uma lista delimitada por vírgulas de volumes a excluir do monitoramento para a política FPolicy à qual o escopo é aplicado.	`-volumes-to-exclude volume_name, ...`
Exportar políticas para incluir Especifica uma lista delimitada por vírgulas de políticas de exportação para monitorar a política FPolicy à qual o escopo é aplicado.	`-export-policies-to -include export_policy_name, ...`
Exportar políticas para excluir Especifica uma lista delimitada por vírgulas de políticas de exportação para excluir do monitoramento da política FPolicy à qual o escopo é aplicado.	`-export-policies-to -exclude export_policy_name, ...`
Extensões de arquivo para incluir Especifica uma lista delimitada por vírgulas de extensões de arquivo para monitorar a política FPolicy à qual o escopo é aplicado.	`-file-extensions-to -include file_extensions, ...`
Extensão de arquivo para excluir Especifica uma lista delimitada por vírgulas de extensões de arquivo para excluir do monitoramento da política FPolicy à qual o escopo é aplicado.	`-file-extensions-to -exclude file_extensions, ...`
A verificação de extensão de arquivo no diretório está ativada ? Especifica se as verificações de extensão de nome de arquivo também se aplicam a objetos de diretório. Se esse parâmetro estiver definido como `true`, os objetos de diretório serão submetidos às mesmas verificações de extensão que os arquivos normais. Se esse parâmetro estiver definido como `false`, os nomes dos diretórios não serão correlacionados para extensões e as notificações serão enviadas para diretórios, mesmo que suas extensões de nome não correspondam. Se a política FPolicy ao qual o escopo é atribuído estiver configurada para usar o mecanismo nativo, esse parâmetro deverá ser definido como `true`.	`-is-file-extension -check-on-directories -enabled{true false`

Preencha a folha de cálculo do escopo da FPolicy

Você pode usar essa Planilha para Registrar os valores necessários durante o processo de configuração do escopo do FPolicy. Se um valor de parâmetro for necessário, você precisará determinar qual valor usar para esses parâmetros antes de configurar o escopo FPolicy.

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do escopo do FPolicy e, em seguida, Registrar o valor dos parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome da política	Sim	Sim	
Compartilhamentos a incluir	Não		
Compartilhamentos a excluir	Não		
Volumes a incluir	Não		
Volumes a excluir	Não		
Políticas de exportação a incluir	Não		
Exportar políticas para excluir	Não		
Extensões de arquivo a incluir	Não		
Extensão do ficheiro a excluir	Não		
A verificação de extensão de arquivo no diretório está ativada?	Não		

Crie a configuração FPolicy

Crie o mecanismo externo FPolicy

Você deve criar um mecanismo externo para começar a criar uma configuração FPolicy. O mecanismo externo define como o FPolicy faz e gerencia conexões com servidores FPolicy externos. Se sua configuração usar o mecanismo interno do ONTAP (o mecanismo externo nativo) para bloqueio de arquivos simples, você não precisará configurar um mecanismo externo FPolicy separado e não precisará executar esta etapa.

O que você vai precisar

A "motor externo" folha de trabalho deve ser concluída.

Sobre esta tarefa

Se o mecanismo externo for usado em uma configuração do MetroCluster, você deverá especificar os endereços IP dos servidores FPolicy no site de origem como servidores primários. Os endereços IP dos servidores FPolicy no local de destino devem ser especificados como servidores secundários.

Passos

1. Crie o mecanismo externo FPolicy usando o `vserver fpolicy policy external-engine create` comando.

   O comando a seguir cria um mecanismo externo na máquina virtual de storage (SVM) vs1.example.com. Não é necessária autenticação para comunicações externas com o servidor FPolicy.

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. Verifique a configuração do mecanismo externo FPolicy usando o `vserver fpolicy policy external-engine show` comando.

   O comando a seguir exibe informações sobre todos os mecanismos externos configurados no SVM vs1.example.com:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                Primary        Secondary
   External
   Vserver            Engine    Servers        Servers       Port Engine
   Type
   ---------------    ----------  -------------- ----------- ------
   -----------
   vs1.example.com    engine1     10.1.1.2,      -             6789
   synchronous
                                  10.1.1.3
   ```

   O comando a seguir exibe informações detalhadas sobre o mecanismo externo chamado "'Engine1" no SVM vs1.example.com:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                            Vserver: vs1.example.com
                             Engine: engine1
             Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

Crie o evento FPolicy

Como parte da criação de uma configuração de política FPolicy, você precisa criar um evento FPolicy. Você associa o evento à política FPolicy quando ele é criado. Um evento define qual protocolo monitorar e quais eventos de acesso ao arquivo monitorar e filtrar.

Antes de começar

Você deve concluir o evento FPolicy "folha de trabalho".

Crie o evento FPolicy

1. Crie o evento FPolicy usando o `vserver fpolicy policy event create` comando.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Verifique a configuração do evento FPolicy usando o `vserver fpolicy policy event show` comando.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                    Event                File                       Is Volume
   Vserver          Name      Protocols  Operations    Filters      Operation
   ---------------  --------- ---------  ------------- ---------
   ------------
   vs1.example.com  event1    cifs       open, close,  -            false
                                         read, write
   ```

Crie os eventos Acesso negado FPolicy

A partir do ONTAP 9.13,1, os usuários podem receber notificações para operações de arquivos com falha devido à falta de permissões. Essas notificações são valiosas para segurança, proteção contra ransomware e governança.

1. Crie o evento FPolicy usando o `vserver fpolicy policy event create` comando.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Criar armazenamentos persistentes FPolicy

Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente. A partir do ONTAP 9.14,1, o FPolicy permite que você configure "armazenamentos persistentes"para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

A partir do ONTAP 9.15,1, a configuração de armazenamento persistente do FPolicy é simplificada. O `persistent-store create` comando automatiza a criação de volume para o SVM e configura o volume para o armazenamento persistente.

Há duas maneiras de criar um armazenamento persistente, dependendo da versão do ONTAP:

- ONTAP 9.15,1 ou posterior: Quando você cria o armazenamento persistente, o ONTAP cria e configura automaticamente seu volume ao mesmo tempo. Isso simplifica a configuração de armazenamento persistente do FPolicy e implementa todas as práticas recomendadas.
- ONTAP 9.14,1: Crie e configure manualmente um volume e, em seguida, crie um armazenamento persistente para o volume recém-criado.

Apenas um armazenamento persistente pode ser configurado em cada SVM. Esse único armazenamento persistente precisa ser usado em todas as configurações de FPolicy nesse SVM, mesmo que as políticas sejam de parceiros diferentes.

Criar um armazenamento persistente (ONTAP 9.15,1 ou posterior)

A partir do ONTAP 9.15,1, use o `fpolicy persistent-store create` comando para criar o armazenamento persistente FPolicy com criação e configuração de volume inline. O ONTAP bloqueia automaticamente o volume do acesso ao protocolo de usuário externo (CIFS/NFS).

Antes de começar

- O SVM em que você deseja criar o armazenamento persistente deve ter pelo menos um agregado.
- Você deve ter acesso aos agregados disponíveis para o SVM e permissões suficientes para criar volumes.

Passos

1. Crie o armazenamento persistente, que cria e configura o volume automaticamente:

   ```
   vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
   <name> -volume <volume_name> -size <size> -autosize-mode
   <off|grow|grow_shrink>
   ```

   - O `vserver` parâmetro é o nome do SVM.
   - O `persistent-store` parâmetro é o nome do armazenamento persistente.
   - O `volume` parâmetro é o nome do volume de armazenamento persistente.

Se você quiser usar um volume vazio existente, use o `volume show` comando para localizá-lo e especificá-lo no parâmetro volume.

- O `size` parâmetro é baseado na duração do tempo para o qual você deseja persistir os eventos que não são entregues ao servidor externo (aplicativo parceiro).

  Por exemplo, se você quiser que 30 minutos de eventos persistam em um cluster com uma capacidade de 30K notificações por segundo:

  Tamanho de volume necessário: 30000 x 30 x 60 x 0,6KB (tamanho médio do Registro de notificação): 32400000 KB, aproximadamente 32 GB

  Para encontrar a taxa de notificação aproximada, você pode entrar em Contato com seu aplicativo de parceiro FPolicy ou utilizar o contador FPolicy `requests_dispatched_rate`.

  Se você estiver usando um volume existente, o parâmetro tamanho é opcional. Se você fornecer um valor para o parâmetro tamanho, ele modificará o volume com o tamanho especificado.

- O `autosize-mode` parâmetro especifica o modo de dimensionamento automático para o volume. Os modos de dimensionamento automático suportados são:
  - Desligado - o volume não cresce nem diminui em tamanho em resposta à quantidade de espaço usado.
  - Crescer - o volume cresce automaticamente quando o espaço usado no volume está acima do limite de crescimento.
  - Grow_shrink - o volume cresce ou encolhe em tamanho em resposta à quantidade de espaço usado.

2. Crie a política FPolicy e adicione o nome do armazenamento persistente a essa política. Para obter mais informações, "Crie a política FPolicy"consulte .

Criar um armazenamento persistente (ONTAP 9.14,1)

Você pode criar um volume e, em seguida, criar um armazenamento persistente para usar esse volume. Em seguida, você pode bloquear o volume recém-criado do acesso de protocolo de usuário externo (CIFS/NFS).

Passos

1. Crie um volume vazio na SVM que possa ser provisionado para o armazenamento persistente:

   ```
   volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
   <default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
   -snapshot-policy <none>
   ```

   Espera-se que um usuário administrador com Privileges RBAC suficiente (para criar um volume) crie um volume (usando o comando da cli de volume ou API REST) do tamanho desejado e forneça o nome desse volume como o `-volume` comando criar CLI no armazenamento persistente ou API REST.

   - O `vserver` parâmetro é o nome do SVM.
   - O `volume` parâmetro é o nome do volume de armazenamento persistente.
   - O `state` parâmetro deve ser definido como online para que o volume esteja disponível para uso.

- O `policy` parâmetro é definido para a política de serviço FPolicy, se você já tiver um configurado. Caso contrário, você pode usar o `volume modify` comando mais tarde para adicionar a política.
- O `unix-permissions` parâmetro é opcional.
- O `size` parâmetro é baseado na duração do tempo para o qual você deseja persistir os eventos que não são entregues ao servidor externo (aplicativo parceiro).

  Por exemplo, se você quiser que 30 minutos de eventos persistam em um cluster com uma capacidade de 30K notificações por segundo:

  Tamanho de volume necessário: 30000 x 30 x 60 x 0,6KB (tamanho médio do Registro de notificação): 32400000 KB, aproximadamente 32 GB

Para encontrar a taxa de notificação aproximada, você pode entrar em Contato com seu aplicativo de parceiro FPolicy ou utilizar o contador FPolicy `requests_dispatched_rate`.

- O parâmetro agregado é necessário para volumes FlexVol, caso contrário não é necessário.
- O `snapshot-policy` parâmetro deve ser definido como nenhum. Isso garante que não haja restauração acidental do snapshot levando à perda de eventos atuais e impede o possível processamento de eventos duplicados.

  Se você quiser usar um volume vazio existente, use o `volume show` comando para encontrá-lo e o `volume modify` comando para fazer as alterações necessárias. Certifique-se de que a política, o tamanho e `snapshot-policy` os parâmetros estão definidos corretamente para o armazenamento persistente.

2. Crie o armazenamento persistente:

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - O `vserver` parâmetro é o nome do SVM.
   - O `persistent-store` parâmetro é o nome do armazenamento persistente.
   - O `volume` parâmetro é o nome do volume de armazenamento persistente.
3. Crie a política FPolicy e adicione o nome do armazenamento persistente a essa política. Para obter mais informações, "Crie a política FPolicy"consulte .

Crie a política FPolicy

Ao criar a política FPolicy, você associa um mecanismo externo e um ou mais eventos à política. A política também especifica se a triagem obrigatória é necessária, se os servidores FPolicy têm acesso privilegiado aos dados na máquina virtual de armazenamento (SVM) e se a leitura de passagem para arquivos off-line está ativada.

O que você vai precisar

- A Planilha de política FPolicy deve ser concluída.
- Se você planeja configurar a política para usar servidores FPolicy, o mecanismo externo deve existir.
- Deve existir pelo menos um evento FPolicy que pretende associar à política FPolicy.
- Se você quiser configurar o acesso a dados privilegiados, um servidor SMB deve existir na SVM.

- Para configurar um armazenamento persistente para uma política, o tipo de mecanismo deve ser **assíncrono** e a política deve ser **não obrigatória**.

  Para obter mais informações, "Crie armazenamentos persistentes"consulte .

Passos

1. Crie a política FPolicy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-persistent-store
   PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
   privileged-user-name domain\user_name] [-is-passthrough-read-enabled
   {true|false}]
   ```

   - Você pode adicionar um ou mais eventos à política FPolicy.
   - Por predefinição, a seleção obrigatória está ativada.
   - Se você quiser permitir acesso privilegiado definindo o `-allow-privileged-access` parâmetro como `yes`, você também deve configurar um nome de usuário privilegiado para acesso privilegiado.
   - Se você quiser configurar a passagem-leitura definindo o `-is-passthrough-read-enabled` parâmetro como `true`, você também deve configurar o acesso privilegiado a dados.

     O comando a seguir cria uma política chamada "policy1" que tem o evento chamado ""event1"" e o motor externo chamado ""Engine1"" associado a ele. Esta política usa valores padrão na configuração da política:
     `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

     O comando a seguir cria uma política chamada "policy2" que tem o evento chamado ""event2"" e o motor externo chamado ""engine2"" associado a ele. Esta política é configurada para usar o acesso privilegiado usando o nome de usuário especificado. A passagem-leitura está ativada:

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
     -events event2 -engine engine2 -allow-privileged-access yes -privileged-
     user-name example\archive_acct -is-passthrough-read-enabled true
     ```

     O comando a seguir cria uma política chamada "'native1" que tem o evento chamado "'event3" associado a ele. Esta política usa o mecanismo nativo e usa valores padrão na configuração da política:

   ```
   vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
   -events event3 -engine native
   ```

2. Verifique a configuração da diretiva FPolicy usando o `vserver fpolicy policy show` comando.

   O comando a seguir exibe informações sobre as três políticas FPolicy configuradas, incluindo as seguintes informações:

   - O SVM associado à política
   - O motor externo associado à política
   - Os eventos associados à política

- Se é necessária uma triagem obrigatória
- Se o acesso privilegiado é necessário
  `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

Crie o escopo FPolicy

Depois de criar a política FPolicy, você precisa criar um escopo FPolicy. Ao criar o escopo, você associa o escopo a uma política FPolicy. Um escopo define os limites nos quais a política FPolicy se aplica. Os escopos podem incluir ou excluir arquivos com base em compartilhamentos, políticas de exportação, volumes e extensões de arquivo.

O que você vai precisar

A folha de trabalho do âmbito da FPolicy tem de ser concluída. A política FPolicy deve existir com um mecanismo externo associado (se a política estiver configurada para usar servidores FPolicy externos) e deve ter pelo menos um evento FPolicy associado.

Passos

1. Crie o escopo FPolicy usando o `vserver fpolicy policy scope create` comando.

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. Verifique a configuração do escopo do FPolicy usando o `vserver fpolicy policy scope show` comando.

   ```
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

Ative a política FPolicy

Depois de configurar uma configuração de política FPolicy, você ativa a política FPolicy. A ativação da política define sua prioridade e inicia o monitoramento de acesso a arquivos para a política.

O que você vai precisar

A política FPolicy deve existir com um mecanismo externo associado (se a política estiver configurada para usar servidores FPolicy externos) e deve ter pelo menos um evento FPolicy associado. O escopo da política FPolicy deve existir e deve ser atribuído à política FPolicy.

Sobre esta tarefa

A prioridade é usada quando várias políticas são habilitadas na máquina virtual de storage (SVM) e mais de uma política é subscrita ao mesmo evento de acesso a arquivos. As políticas que usam a configuração nativa do mecanismo têm uma prioridade maior do que as políticas para qualquer outro mecanismo, independentemente do número de sequência atribuído a elas ao ativar a política.

Não é possível ativar uma política no SVM do administrador.

Passos

1. Ative a política FPolicy usando o `vserver fpolicy enable` comando.

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. Verifique se a política FPolicy está ativada usando o `vserver fpolicy show` comando.

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                    Sequence
   Vserver          Policy Name       Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                1  on       engine1
   ```

Gerenciar configurações de FPolicy

Modificar configurações FPolicy

Comandos para modificar configurações FPolicy

Você pode modificar as configurações do FPolicy modificando os elementos que compõem a configuração. Você pode modificar mecanismos externos, eventos FPolicy, escopos FPolicy, armazenamentos persistentes FPolicy e políticas FPolicy. Você também pode ativar ou desativar políticas FPolicy. Quando você desativa a política FPolicy, o monitoramento de arquivos é descontinuado para essa política.

Você deve desativar uma política FPolicy antes de modificar sua configuração.

Se você quiser modificar…	Use este comando…
Motores externos	`vserver fpolicy policy external-engine modify`
Eventos	`vserver fpolicy policy event modify`
Escopos	`vserver fpolicy policy scope modify`
Armazenamento persistente	`vserver fpolicy persistent-store modify`
Políticas	`vserver fpolicy policy modify`

Consulte as páginas de manual para obter mais informações.

Ativar ou desativar políticas FPolicy

Você pode ativar as políticas FPolicy após a conclusão da configuração. A ativação da política define sua prioridade e inicia o monitoramento de acesso a arquivos para a política. Você pode desativar as políticas FPolicy se quiser interromper o monitoramento de acesso a arquivos para a política.

O que você vai precisar

Antes de ativar as políticas FPolicy, a configuração FPolicy deve ser concluída.

Sobre esta tarefa

- A prioridade é usada quando várias políticas são habilitadas na máquina virtual de storage (SVM) e mais de uma política é subscrita ao mesmo evento de acesso a arquivos.
- As políticas que usam a configuração nativa do mecanismo têm uma prioridade maior do que as políticas para qualquer outro mecanismo, independentemente do número de sequência atribuído a elas ao ativar a política.
- Se pretender alterar a prioridade de uma política FPolicy, tem de desativar a política e, em seguida, reactivá-la utilizando o novo número de sequência.

Passo

1. Execute a ação apropriada:

Se você quiser…	Digite o seguinte comando…
Ativar uma política FPolicy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Desativar uma política FPolicy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Exibir informações sobre as configurações do FPolicy

Como funcionam os comandos show

É útil ao exibir informações sobre a configuração do FPolicy para entender como os `show` comandos funcionam.

Um `show` comando sem parâmetros adicionais exibe informações em um formulário de resumo. Além disso, cada `show` comando tem os mesmos dois parâmetros opcionais mutuamente exclusivos, `-instance` e `-fields`.

Quando você usa o `-instance` parâmetro com um `show` comando, a saída do comando exibe informações detalhadas em um formato de lista. Em alguns casos, a saída detalhada pode ser longa e incluir mais informações do que você precisa. Você pode usar o `-fields fieldname[,fieldname…]` parâmetro para personalizar a saída para que ela exiba informações apenas para os campos especificados. Você pode identificar quais campos você pode especificar inserindo `?` após o `-fields` parâmetro.

> A saída de um `show` comando com o `-fields` parâmetro pode exibir outros campos relevantes e necessários relacionados aos campos solicitados.

Cada `show` comando tem um ou mais parâmetros opcionais que filtram essa saída e permitem restringir o escopo das informações exibidas na saída de comando. Você pode identificar quais parâmetros opcionais estão disponíveis para um comando inserindo `?` após o `show` comando.

O `show` comando suporta padrões de estilo UNIX e wildcards para permitir que você combine vários valores em argumentos de parâmetros de comando. Por exemplo, você pode usar o operador curinga (*), o operador NÃO (!), o OPERADOR OR (|), o operador de intervalo (integer…integer), o operador menor (>), o operador maior (>), o operador menor ou igual ao operador (>) e o operador maior ou igual a (>) ao especificar valores.

Para obter mais informações sobre como usar padrões e curingas de estilo UNIX, consulte Usando a interface de linha de comando ONTAP.

Comandos para exibir informações sobre configurações FPolicy

Você usa os `fpolicy show` comandos para exibir informações sobre a configuração do FPolicy, incluindo informações sobre mecanismos externos, eventos, escopos e políticas do FPolicy.

Se você quiser exibir informações sobre FPolicy…	Use este comando…
Motores externos	`vserver fpolicy policy external-engine show`
Eventos	`vserver fpolicy policy event show`
Escopos	`vserver fpolicy policy scope show`
Políticas	`vserver fpolicy policy show`

Consulte as páginas de manual para obter mais informações.

Exibir informações sobre o status da política FPolicy

Você pode exibir informações sobre o status das políticas FPolicy para determinar se uma política está ativada, qual mecanismo externo ele está configurado para usar, qual é o número de sequência para a política e a qual máquina virtual de armazenamento (SVM) a política FPolicy está associada.

Sobre esta tarefa

Se você não especificar nenhum parâmetro, o comando exibirá as seguintes informações:

- Nome do SVM
- Nome da política
- Número de sequência da política
- Estado da política

Além de exibir informações sobre o status da política para políticas FPolicy configuradas no cluster ou em um SVM específico, você pode usar parâmetros de comando para filtrar a saída do comando por outros critérios.

Você pode especificar o `-instance` parâmetro para exibir informações detalhadas sobre as políticas listadas. Alternativamente, você pode usar o `-fields` parâmetro para exibir apenas os campos indicados na saída do comando ou `-fields ?` para determinar quais campos você pode usar.

Passo

1. Exiba informações filtradas sobre o status da política FPolicy usando o comando apropriado:

Se você quiser exibir informações de status sobre políticas…	Digite o comando…
No cluster	`vserver fpolicy show`
Que têm o status especificado	`vserver fpolicy show -status {on`
off}`	Em uma SVM especificada
`vserver fpolicy show -vserver vserver_name`	Com o nome da política especificado
`vserver fpolicy show -policy-name policy_name`	Que utilizam o motor externo especificado

Exemplo

O exemplo a seguir exibe as informações sobre políticas FPolicy no cluster:

```
cluster1::> vserver fpolicy show
                                        Sequence
Vserver              Policy Name          Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy       -         off         eng1
vs1.example.com      v1p1                 -         off         eng2
vs1.example.com      v1p2                 -         off         native
vs1.example.com      v1p3                 -         off         native
vs1.example.com      cserver_policy       -         off         eng1
vs2.example.com      v1p1                 3         on          native
vs2.example.com      v1p2                 1         on          eng3
vs2.example.com      cserver_policy       2         on          eng1
```

Exibir informações sobre políticas FPolicy ativadas

Você pode exibir informações sobre políticas FPolicy ativadas para determinar qual mecanismo externo FPolicy ele está configurado para usar, qual é a prioridade para a política e a qual máquina virtual de armazenamento (SVM) a política FPolicy está associada.

Sobre esta tarefa

Se você não especificar nenhum parâmetro, o comando exibirá as seguintes informações:

- Nome do SVM
- Nome da política
- Prioridade da política

Você pode usar parâmetros de comando para filtrar a saída do comando por critérios especificados.

Passo

1. Exiba informações sobre políticas FPolicy ativadas usando o comando apropriado:

Se você quiser exibir informações sobre políticas ativadas…	Digite o comando…
No cluster	`vserver fpolicy show-enabled`
Em uma SVM especificada	`vserver fpolicy show-enabled -vserver vserver_name`
Com o nome da política especificado	`vserver fpolicy show-enabled -policy-name policy_name`
Com o número de sequência especificado	`vserver fpolicy show-enabled -priority integer`

Exemplo

O exemplo a seguir exibe as informações sobre as políticas FPolicy ativadas no cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

Gerenciar conexões do servidor FPolicy

Conete-se a servidores FPolicy externos

Para habilitar o processamento de arquivos, talvez seja necessário conetar-se manualmente a um servidor FPolicy externo se a conexão tiver sido encerrada anteriormente. Uma conexão é terminada após o tempo limite do servidor ser atingido ou devido a algum erro. Como alternativa, o administrador pode encerrar manualmente uma conexão.

Sobre esta tarefa

Se ocorrer um erro fatal, a conexão com o servidor FPolicy pode ser encerrada. Depois de resolver o problema que causou o erro fatal, você deve se reconetar manualmente ao servidor FPolicy.

Passos

1. Conete-se ao servidor FPolicy externo usando o `vserver fpolicy engine-connect` comando.

   Para obter mais informações sobre o comando, consulte as páginas de manual.

2. Verifique se o servidor FPolicy externo está conetado usando o `vserver fpolicy show-engine` comando.

   Para obter mais informações sobre o comando, consulte as páginas de manual.

Desconetar de servidores FPolicy externos

Talvez seja necessário desconetar manualmente de um servidor FPolicy externo. Isso pode ser desejável se o servidor FPolicy tiver problemas com o processamento de solicitação de notificação ou se você precisar executar manutenção no servidor FPolicy.

Passos

1. Desconete do servidor FPolicy externo usando o `vserver fpolicy engine-disconnect` comando.

   Para obter mais informações sobre o comando, consulte as páginas de manual.

2. Verifique se o servidor FPolicy externo está desconetado usando o `vserver fpolicy show-engine` comando.

Para obter mais informações sobre o comando, consulte as páginas de manual.

Exibir informações sobre conexões com servidores FPolicy externos

Você pode exibir informações de status sobre conexões com servidores FPolicy externos (servidores FPolicy) para o cluster ou para uma máquina virtual de armazenamento especificada (SVM). Essas informações podem ajudá-lo a determinar quais servidores FPolicy estão conetados.

Sobre esta tarefa

Se você não especificar nenhum parâmetro, o comando exibirá as seguintes informações:

- Nome do SVM
- Nome do nó
- Nome da política FPolicy
- Endereço IP do servidor FPolicy
- Status do servidor FPolicy
- Tipo de servidor FPolicy

Além de exibir informações sobre conexões FPolicy no cluster ou em um SVM específico, você pode usar parâmetros de comando para filtrar a saída do comando por outros critérios.

Você pode especificar o `-instance` parâmetro para exibir informações detalhadas sobre as políticas listadas. Alternativamente, você pode usar o `-fields` parâmetro para exibir apenas os campos indicados na saída do comando. Você pode inserir `?` após o `-fields` parâmetro para descobrir quais campos você pode usar.

Passo

1. Exiba informações filtradas sobre o status da conexão entre o nó e o servidor FPolicy usando o comando apropriado:

Se você quiser exibir informações de status de conexão sobre servidores FPolicy…	Digite…
Que você especificar	`vserver fpolicy show-engine -server IP_address`
Para uma SVM especificada	`vserver fpolicy show-engine -vserver vserver_name`
Que estão anexados a uma política especificada	`vserver fpolicy show-engine -policy-name policy_name`

Com o status do servidor especificado	`vserver fpolicy show-engine -server-status status` O status do servidor pode ser um dos seguintes: • `connected` • `disconnected` • `connecting` • `disconnecting`
Com o tipo especificado	`vserver fpolicy show-engine -server-type type` O tipo de servidor FPolicy pode ser um dos seguintes: • `primary` • `secondary`
Que foram desconetadas com o motivo especificado	`vserver fpolicy show-engine -disconnect-reason text` A desconexão pode ser devido a vários motivos. As seguintes razões são comuns para desconetar: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Exemplo

Este exemplo exibe informações sobre conexões externas do mecanismo a servidores FPolicy no SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

Este exemplo exibe informações somente sobre servidores FPolicy conetados:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

Exibir informações sobre o status da conexão de leitura de passagem FPolicy

Você pode exibir informações sobre o status da conexão de leitura de passagem FPolicy para servidores FPolicy externos (servidores FPolicy) para o cluster ou para uma máquina virtual de armazenamento especificada (SVM). Essas informações podem ajudá-lo a determinar quais servidores FPolicy têm conexões de dados de leitura de passagem e para quais servidores FPolicy a conexão de leitura de passagem está desconetada.

Sobre esta tarefa

Se você não especificar nenhum parâmetro, o comando exibirá as seguintes informações:

- Nome do SVM
- Nome da política FPolicy
- Nome do nó
- Endereço IP do servidor FPolicy
- Status da conexão de leitura de passagem de FPolicy

Além de exibir informações sobre conexões FPolicy no cluster ou em um SVM específico, você pode usar parâmetros de comando para filtrar a saída do comando por outros critérios.

Você pode especificar o `-instance` parâmetro para exibir informações detalhadas sobre as políticas listadas. Alternativamente, você pode usar o `-fields` parâmetro para exibir apenas os campos indicados na saída do comando. Você pode inserir `?` após o `-fields` parâmetro para descobrir quais campos você pode usar.

Passo

1. Exiba informações filtradas sobre o status da conexão entre o nó e o servidor FPolicy usando o comando apropriado:

Se pretender apresentar informações sobre o estado da ligação…	Digite o comando…
Status de conexão de leitura de passagem FPolicy para o cluster	`vserver fpolicy show-passthrough-read-connection`
Status de conexão de leitura de passagem de FPolicy para uma SVM especificada	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
Status de conexão de leitura de passagem de FPolicy para uma política especificada	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
Status de conexão de leitura de passagem FPolicy detalhado para uma política especificada	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
Status da conexão de leitura de passagem de FPolicy para o status que você especificar	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` O status do servidor pode ser um dos seguintes: • `connected` • `disconnected`

Exemplo

O comando a seguir exibe informações sobre conexões de leitura de passagem de todos os servidores FPolicy no cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------- ---------- ----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

O comando a seguir exibe informações detalhadas sobre conexões de leitura de passagem de servidores FPolicy configurados na política "'pol_cifs_1":

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                          Node: FPolicy-01
                                       Vserver: vs1.example.com
                                        Policy: pol_cifs_1
                                        Server: 1.1.1.1
                 Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                  Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

Verifique o acesso usando rastreamento de segurança

Como os rastreamentos de segurança funcionam

Você pode adicionar filtros de rastreamento de permissões para instruir o ONTAP a Registrar informações sobre por que os servidores SMB e NFS em uma máquina virtual de armazenamento (SVM) permitem ou negam uma solicitação de cliente ou usuário para executar uma operação. Isso pode ser útil quando você quiser verificar se o esquema de segurança de acesso ao arquivo é apropriado ou quando você deseja solucionar problemas de acesso ao arquivo.

Os rastreamentos de segurança permitem configurar um filtro que deteta operações de clientes em SMB e NFS na SVM e rastrear todas as verificações de acesso correspondentes a esse filtro. Em seguida, é possível visualizar os resultados do rastreio, que fornece um resumo conveniente do motivo pelo qual o acesso foi permitido ou negado.

Quando você deseja verificar as configurações de segurança para acesso SMB ou NFS em arquivos e pastas no SVM ou se você tiver um problema de acesso, você pode adicionar rapidamente um filtro para ativar o rastreamento de permissões.

A lista a seguir descreve fatos importantes sobre como o rastreamento de segurança funciona:

- O ONTAP aplica rastreios de segurança no nível da SVM.
- Cada solicitação recebida é rastreada para ver se corresponde aos critérios de filtragem de quaisquer rastreamentos de segurança ativados.
- Os rastreamentos são executados para solicitações de acesso a arquivos e pastas.
- Os rastreamentos podem filtrar com base nos seguintes critérios:
  - IP do cliente
  - Caminho SMB ou NFS
  - Nome do Windows
  - Nome UNIX

- As solicitações são rastreadas para os resultados da resposta de acesso *allowed* e *denied*.
- Cada pedido que corresponde aos critérios de filtragem de traçados ativados é registado no registo de resultados do rastreio.
- O administrador de armazenamento pode configurar um tempo limite em um filtro para desativá-lo automaticamente.
- Se uma solicitação corresponder a vários filtros, os resultados do filtro com o número de índice mais alto serão registrados.
- O administrador de armazenamento pode imprimir os resultados do registo de resultados do rastreio para determinar por que motivo uma solicitação de acesso foi permitida ou negada.

Tipos de acesso verifica o monitor de rastreios de segurança

As verificações de acesso para um ficheiro ou pasta são efetuadas com base em vários critérios. Os rastreamentos de segurança monitoram as operações em todos esses critérios.

Os tipos de verificações de acesso que os rastreios de segurança monitoram incluem o seguinte:

- Estilo de segurança de volume e qtree
- Segurança efetiva do sistema de arquivos que contém os arquivos e pastas em que as operações são solicitadas
- Mapeamento do utilizador
- Permissões de nível de compartilhamento
- Permissões de nível de exportação
- Permissões no nível do arquivo
- Segurança do Access Guard no nível de storage

Considerações ao criar rastreamentos de segurança

Você deve ter várias considerações em mente quando criar rastreamentos de segurança em máquinas virtuais de armazenamento (SVMs). Por exemplo, você precisa saber em quais protocolos você pode criar um rastreamento, quais estilos de segurança são suportados e qual é o número máximo de rastreamentos ativos.

- Você só pode criar rastreamentos de segurança em SVMs.
- Cada entrada de filtro de rastreamento de segurança é específica da SVM.

  Você deve especificar o SVM no qual deseja executar o rastreamento.

- Você pode adicionar filtros de rastreamento de permissões para solicitações SMB e NFS.
- É necessário configurar o servidor SMB ou NFS no SVM no qual você deseja criar filtros de rastreamento.
- Você pode criar rastreamentos de segurança para arquivos e pastas residentes em NTFS, UNIX e volumes e qtrees mistos de estilo de segurança.
- Você pode adicionar um máximo de 10 filtros de rastreamento de permissões por SVM.
- Você deve especificar um número de índice de filtro ao criar ou modificar um filtro.

Os filtros são considerados pela ordem do número do índice. Os critérios em um filtro com um número de índice mais alto são considerados antes dos critérios com um número de índice mais baixo. Se a solicitação rastreada corresponder a critérios em vários filtros ativados, somente o filtro com o número de índice mais alto será acionado.

- Depois de criar e ativar um filtro de rastreio de segurança, tem de executar algumas solicitações de ficheiro ou pasta num sistema cliente para gerar atividade que o filtro de rastreio pode capturar e iniciar sessão no registo de resultados do rastreio.
- Você deve adicionar filtros de rastreamento de permissões apenas para fins de verificação de acesso a arquivos ou solução de problemas.

  Adicionar filtros de rastreamento de permissões tem um efeito menor no desempenho do controlador.

  Quando terminar com a atividade de verificação ou solução de problemas, desative ou remova todos os filtros de rastreamento de permissões. Além disso, os critérios de filtragem selecionados devem ser o mais específicos possível para que o ONTAP não envie um grande número de resultados de rastreamento para o log.

Execute rastreamentos de segurança

Execute uma visão geral dos rastreamentos de segurança

A execução de um rastreamento de segurança envolve a criação de um filtro de rastreamento de segurança, a verificação dos critérios de filtro, a geração de solicitações de acesso em um cliente SMB ou NFS que correspondam aos critérios de filtro e a visualização dos resultados.

Depois de terminar de usar um filtro de segurança para capturar informações de rastreamento, você pode modificar o filtro e reutilizá-lo ou desativá-lo se não precisar mais dele. Depois de visualizar e analisar os resultados do rastreamento do filtro, você pode excluí-los se eles não forem mais necessários.

Crie filtros de rastreamento de segurança

Você pode criar filtros de rastreamento de segurança que detetam operações de clientes SMB e NFS em máquinas virtuais de armazenamento (SVMs) e rastrear todas as verificações de acesso correspondentes ao filtro. Você pode usar os resultados de rastreamentos de segurança para validar sua configuração ou para solucionar problemas de acesso.

Sobre esta tarefa

Existem dois parâmetros necessários para o comando criar filtro de rastreamento de segurança vserver:

Parâmetros necessários	Descrição
`-vserver vserver_name`	*Nome da SVM* O nome do SVM que contém os arquivos ou pastas em que você deseja aplicar o filtro de rastreamento de segurança.

`-index index_number`	*Número do índice do filtro* O número de índice que você deseja aplicar ao filtro. Você está limitado a um máximo de 10 filtros de rastreamento por SVM. Os valores permitidos para este parâmetro são de 1 a 10.

Vários parâmetros de filtro opcionais permitem personalizar o filtro de rastreamento de segurança para que você possa reduzir os resultados produzidos pelo rastreamento de segurança:

Parâmetro do filtro	Descrição
`-client-ip IP_Address`	Esse filtro especifica o endereço IP a partir do qual o usuário está acessando o SVM.
`-path path`	Este filtro especifica o caminho no qual aplicar o filtro de rastreamento de permissões. O valor para `-path` pode utilizar um dos seguintes formatos: • O caminho completo, a partir da raiz do compartilhamento ou exportação • Um caminho parcial, relativo à raiz do compartilhamento Você deve usar separadores de diretório estilo NFS no valor do caminho.
`-windows-name win_user_name` ou `-unix -name``unix_user_name`	Você pode especificar o nome de usuário do Windows ou o nome de usuário UNIX cujas solicitações de acesso você deseja rastrear. A variável de nome de usuário é insensível a maiúsculas e minúsculas. Não é possível especificar um nome de usuário do Windows e um nome de usuário UNIX no mesmo filtro. Mesmo que você possa rastrear eventos de acesso SMB e NFS, o usuário UNIX mapeado e os grupos de usuários UNIX mapeados podem ser usados ao executar verificações de acesso em dados de estilo de segurança misto ou UNIX.
`-trace-allow {yes`	`no`Selecione
O rastreamento para eventos de negação é sempre ativado para um filtro de rastreamento de segurança. Opcionalmente, você pode rastrear eventos de permissão. Para rastrear eventos de permissão, defina este parâmetro como `yes`.	`-enabled {enabled`
`disabled`Selecione	Pode ativar ou desativar o filtro de rastreio de segurança. Por predefinição, o filtro de rastreio de segurança está ativado.

`-time-enabled integer`	Você pode especificar um tempo limite para o filtro, após o qual ele é desativado.

Passos

1. Criar um filtro de rastreamento de segurança:

   `vserver security trace filter create -vserver vserver_name -index index_numberfilter_parameters`

   `filter_parameters` é uma lista de parâmetros de filtro opcionais.

   Para obter mais informações, consulte as páginas man para o comando.

2. Verifique a entrada do filtro de rastreamento de segurança:

   `vserver security trace filter show -vserver vserver_name -index index_number`

Exemplos

O comando a seguir cria um filtro de rastreamento de segurança para qualquer usuário que acesse um arquivo com um caminho de compartilhamento do `\\server\share1\dir1\dir2\file.txt` endereço IP 10.10.10.7. O filtro usa um caminho completo para a `-path` opção. O endereço IP do cliente usado para acessar dados é 10.10.10.7. O filtro expira após 30 minutos:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

O comando a seguir cria um filtro de rastreamento de segurança usando um caminho relativo para a `-path` opção. O filtro rastreia o acesso de um usuário do Windows chamado "joe". Joe está acessando um arquivo com um caminho de compartilhamento `\\server\share1\dir1\dir2\file.txt` . Os rastreamentos de filtro permitem e negam eventos:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: mydomain\joe
                        UNIX User Name: -
                     Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Exibir informações sobre filtros de rastreamento de segurança

Você pode exibir informações sobre filtros de rastreamento de segurança configurados na máquina virtual de armazenamento (SVM). Isso permite que você veja quais tipos de eventos de acesso cada filtro rastreia.

Passo

1. Exiba informações sobre entradas de filtro de rastreamento de segurança usando o `vserver security trace filter show` comando.

   Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Exemplos

O comando a seguir exibe informações sobre todos os filtros de rastreamento de segurança no SVM VS1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Apresentar resultados do rastreio de segurança

Você pode exibir os resultados do rastreamento de segurança gerados para operações de arquivo que correspondam aos filtros de rastreamento de segurança. Use os resultados para validar a configuração de segurança de acesso a arquivos ou para solucionar problemas de acesso a arquivos SMB e NFS.

O que você vai precisar

Um filtro de rastreamento de segurança habilitado deve existir e as operações devem ter sido executadas a partir de um cliente SMB ou NFS que corresponda ao filtro de rastreamento de segurança para gerar resultados de rastreamento de segurança.

Sobre esta tarefa

Você pode exibir um resumo de todos os resultados do rastreamento de segurança ou personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando os resultados do rastreamento de segurança contêm um grande número de Registros.

Se não especificar nenhum dos parâmetros opcionais, é apresentado o seguinte:

- Nome da máquina virtual de storage (SVM)
- Nome do nó
- Número do índice de rastreamento de segurança
- Estilo de segurança
- Caminho
- Motivo
- Nome de utilizador

  O nome de utilizador é apresentado consoante a configuração do filtro de rastreio:

Se o filtro estiver configurado…	Então…
Com um nome de usuário UNIX	O resultado do rastreamento de segurança exibe o nome de usuário UNIX.
Com um nome de usuário do Windows	O resultado do rastreamento de segurança exibe o nome de usuário do Windows.
Sem um nome de usuário	O resultado do rastreamento de segurança exibe o nome de usuário do Windows.

Você pode personalizar a saída usando parâmetros opcionais. Alguns dos parâmetros opcionais que você pode usar para restringir os resultados retornados na saída do comando incluem o seguinte:

Parâmetro opcional	Descrição
`-fields field_name, ...`	Exibe a saída nos campos que você escolher. Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.
`-instance`	Exibe informações detalhadas sobre eventos de rastreamento de segurança. Use este parâmetro com outros parâmetros opcionais para exibir informações detalhadas sobre os resultados específicos do filtro.
`-node node_name`	Exibe informações somente sobre eventos no nó especificado.

`-vserver vserver_name`	Exibe informações somente sobre eventos na SVM especificada.
`-index integer`	Exibe informações sobre os eventos que ocorreram como resultado do filtro correspondente ao número de índice especificado.
`-client-ip IP_address`	Exibe informações sobre os eventos que ocorreram como resultado do acesso ao arquivo a partir do endereço IP do cliente especificado.
`-path path`	Exibe informações sobre os eventos que ocorreram como resultado do acesso de arquivos ao caminho especificado.
`-user-name user_name`	Exibe informações sobre os eventos que ocorreram como resultado do acesso a arquivos pelo usuário especificado do Windows ou UNIX.
`-security-style security_style`	Exibe informações sobre os eventos ocorridos em sistemas de arquivos com o estilo de segurança especificado.

Consulte a página man para obter informações sobre outros parâmetros opcionais que você pode usar com o comando.

Passo

1. Exiba os resultados do filtro de rastreamento de segurança usando o `vserver security trace trace-result show` comando.

   ```
   vserver security trace trace-result show -user-name domain\user
   ```

   ```
   Vserver: vs1

   Node     Index   Filter Details         Reason
   -------- ------- ---------------------  ------------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

Modificar filtros de rastreamento de segurança

Se você quiser alterar os parâmetros de filtro opcionais usados para determinar quais eventos de acesso são rastreados, você pode modificar os filtros de rastreamento de segurança existentes.

Sobre esta tarefa

Você deve identificar qual filtro de rastreamento de segurança deseja modificar especificando o nome da máquina virtual de armazenamento (SVM) no qual o filtro é aplicado e o número de índice do filtro. Você pode modificar todos os parâmetros de filtro opcionais.

Passos

1. Modificar um filtro de rastreamento de segurança:

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name` É o nome do SVM no qual você deseja aplicar um filtro de rastreamento de segurança.
   - `index_number` é o número de índice que você deseja aplicar ao filtro. Os valores permitidos para este parâmetro são de 1 a 10.
   - `filter_parameters` é uma lista de parâmetros de filtro opcionais.

2. Verifique a entrada do filtro de rastreamento de segurança:

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

Exemplo

O comando a seguir modifica o filtro de rastreamento de segurança com o índice número 1. O filtro rastreia eventos para qualquer usuário acessando um arquivo com um caminho de compartilhamento `\\server\share1\dir1\dir2\file.txt` a partir de qualquer endereço IP. O filtro usa um caminho completo para a `-path` opção. Os rastreamentos de filtro permitem e negam eventos:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                              Vserver: vs1
                         Filter Index: 1
             Client IP Address to Match: -
                                 Path: /dir1/dir2/file.txt
                  Windows User Name: -
                     UNIX User Name: -
                   Trace Allow Events: yes
                      Filter Enabled: enabled
              Minutes Filter is Enabled: 60
```

Excluir filtros de rastreamento de segurança

Quando você não precisa mais de uma entrada de filtro de rastreamento de segurança, você pode excluí-lo. Como você pode ter um máximo de 10 filtros de rastreamento de segurança por máquina virtual de armazenamento (SVM), excluir filtros desnecessários permite criar novos filtros se você atingir o máximo.

Sobre esta tarefa

Para identificar de forma exclusiva o filtro de rastreamento de segurança que você deseja excluir, você deve especificar o seguinte:

- O nome do SVM ao qual o filtro de rastreamento é aplicado
- O número do índice do filtro do traçado

Passos

1. Identifique o número do índice do filtro da entrada do filtro de rastreamento de segurança que você deseja excluir:

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. Usando as informações do número do índice do filtro da etapa anterior, exclua a entrada do filtro:

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number

   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Verifique se a entrada do filtro de rastreamento de segurança foi excluída:

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

Eliminar registos de rastreio de segurança

Depois de terminar de usar um Registro de rastreamento de filtro para verificar a segurança do acesso ao arquivo ou para solucionar problemas de acesso ao cliente SMB ou NFS, você pode excluir o Registro de rastreamento de segurança do log de rastreamento de segurança.

Sobre esta tarefa

Antes de poder eliminar um registo de rastreio de segurança, tem de saber o número de sequência do registo.

> Cada máquina virtual de storage (SVM) pode armazenar no máximo 128 Registros de rastreamento. Se o máximo for atingido na SVM, os Registros de rastreamento mais antigos serão excluídos automaticamente à medida que novos forem adicionados. Se você não quiser excluir manualmente os Registros de rastreamento neste SVM, você pode permitir que o ONTAP exclua automaticamente os resultados de rastreamento mais antigos depois que o máximo for atingido para abrir espaço para novos resultados.

Passos

1. Identifique o número de sequência do registo que pretende eliminar:

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. Eliminar o registo de rastreio de segurança:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer
   ```

   ```
   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node node_name` é o nome do nó do cluster no qual ocorreu o evento de rastreamento de permissões que você deseja excluir.

     Este é um parâmetro obrigatório.

   - `-vserver vserver_name` É o nome do SVM no qual ocorreu o evento de rastreamento de permissões que você deseja excluir.

     Este é um parâmetro obrigatório.

   - `-seqnum integer` é o número de sequência do evento de registo que pretende eliminar.

     Este é um parâmetro obrigatório.

Eliminar todos os registos de rastreio de segurança

Se você não quiser manter nenhum dos Registros de rastreamento de segurança existentes, você pode excluir todos os Registros em um nó com um único comando.

Passo

1. Eliminar todos os registos de rastreio de segurança:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - `-node node_name` é o nome do nó do cluster no qual ocorreu o evento de rastreamento de permissões que você deseja excluir.
   - `-vserver vserver_name` É o nome da máquina virtual de armazenamento (SVM) na qual ocorreu o

evento de rastreamento de permissões que você deseja excluir.

Interpretar os resultados do rastreamento de segurança

Os resultados do rastreamento de segurança fornecem o motivo pelo qual uma solicitação foi permitida ou negada. A saída exibe o resultado como uma combinação do motivo para permitir ou negar acesso e o local dentro do caminho de verificação de acesso onde o acesso é permitido ou negado. Você pode usar os resultados para isolar e identificar por que as ações são ou não permitidas.

Encontrar informações sobre as listas de tipos de resultados e detalhes do filtro

Você pode encontrar as listas de tipos de resultados e detalhes de filtro que podem ser incluídos nos resultados de rastreamento de segurança nas páginas de manual do `vserver security trace trace-result show` comando.

Exemplo de saída do `Reason` campo em um `Allow` tipo de resultado

O seguinte é um exemplo da saída do `Reason` campo que aparece no log de resultados do rastreamento em um `Allow` tipo de resultado:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

Exemplo de saída do `Reason` campo em um `Allow` tipo de resultado

O seguinte é um exemplo da saída do `Reason` campo que aparece no log de resultados do rastreamento em um `Deny` tipo de resultado:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Exemplo de saída do `Filter details` campo

A seguir está um exemplo da saída do `Filter details` campo no log de resultados do rastreamento, que lista o estilo de segurança efetivo do sistema de arquivos contendo arquivos e pastas que correspondem aos critérios do filtro:

```
Security Style: MIXED and ACL
```

Onde encontrar informações adicionais

Depois de testar o acesso de cliente SMB com sucesso, você pode executar a

configuração SMB avançada ou adicionar acesso SAN. Depois de testar com êxito o acesso ao cliente NFS, você pode executar uma configuração NFS avançada ou adicionar acesso SAN. Quando o acesso ao protocolo for concluído, você deverá proteger o volume raiz da SVM.

Configuração SMB

Você pode configurar ainda mais o acesso SMB usando o seguinte:

- "Gerenciamento de SMB"

  Descreve como configurar e gerenciar o acesso a arquivos usando o protocolo SMB.

- "Relatório técnico da NetApp 4191: Guia de práticas recomendadas para Serviços de arquivos do Windows Clustered Data ONTAP 8.2"

  Fornece uma breve visão geral da implementação de SMB e outros recursos de Serviços de arquivos do Windows com recomendações e informações básicas de solução de problemas para o ONTAP.

- "Relatório técnico da NetApp 3740: Protocolo CIFS de última geração SMB 2 no Data ONTAP"

  Descreve os recursos do SMB 2, detalhes de configuração e sua implementação no ONTAP.

Configuração NFS

Você pode configurar ainda mais o acesso NFS usando o seguinte:

- "Gerenciamento de NFS"

  Descreve como configurar e gerenciar o acesso a arquivos usando o protocolo NFS.

- "Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"

  Serve como um guia operacional NFSv3 e NFSv4 e fornece uma visão geral do sistema operacional ONTAP com foco em NFSv4.

- "Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

  Fornece uma lista abrangente de práticas recomendadas, limites, recomendações e considerações ao configurar LDAP, NIS, DNS e arquivos de usuário e grupo locais para fins de autenticação.

- "Relatório técnico do NetApp 4616: Kerberos NFS no ONTAP com o Microsoft ative Directory"
- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"
- "Relatório técnico da NetApp 3580: NFSv4 melhorias e melhores práticas Guia de implementação do Data ONTAP"

  Descreve as práticas recomendadas que devem ser seguidas durante a implementação de componentes NFSv4 em clientes AIX, Linux ou Solaris conetados a sistemas que executam o ONTAP.

Proteção do volume raiz

Depois de configurar protocolos no SVM, você deve garantir que seu volume raiz esteja protegido:

- "Proteção de dados"

  Descreve como criar um espelhamento de compartilhamento de carga para proteger o volume raiz da SVM, que é uma prática recomendada do NetApp para SVMs habilitadas para nas. Também descreve como recuperar rapidamente de falhas ou perdas de volume promovendo o volume raiz do SVM a partir de um espelhamento de compartilhamento de carga.

Gerencie a criptografia com o System Manager

Criptografe dados armazenados usando criptografia baseada em software

Use a criptografia de volume para garantir que os dados de volume não possam ser lidos se o dispositivo subjacente for reutilizado, retornado, extraviado ou roubado. A criptografia de volume não requer discos especiais; ela funciona com todos os HDDs e SSDs.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para ativar a encriptação no nível do software. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A criptografia de volumes requer um gerenciador de chaves. Você pode configurar o Gerenciador de chaves integrado usando o System Manager. Você também pode usar um gerenciador de chaves externo, mas primeiro precisa configurá-lo usando a CLI do ONTAP.

Depois que o gerenciador de chaves é configurado, novos volumes são criptografados por padrão.

Passos

1. Clique em **Cluster > Settings**.
2. Em **Encryption**, clique para configurar o Onboard Key Manager pela primeira vez.
3. Para encriptar volumes existentes, clique em **armazenamento > volumes**.
4. No volume desejado, clique em **Edit** (Editar).
5. Selecione **Ativar encriptação**.

Criptografe dados armazenados usando unidades com autocriptografia

Use a criptografia de disco para garantir que todos os dados em um nível local não possam ser lidos se o dispositivo subjacente for reutilizado, retornado, extraviado ou roubado. A criptografia de disco requer HDDs ou SSDs especiais com autocriptografia.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para ativar a criptografia no nível de hardware. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A criptografia de disco requer um gerenciador de chaves. Você pode configurar o gerenciador de chaves integrado usando o System Manager. Você também pode usar um gerenciador de chaves externo, mas primeiro precisa configurá-lo usando a CLI do ONTAP.

Se o ONTAP detetar discos com autocriptografia, ele solicitará que você configure o gerenciador de chaves integrado ao criar o nível local.

Passos

1. Em **Encryption**, clique para configurar o gerenciador de chaves integrado.
2. Se você vir uma mensagem informando que os discos precisam ser rekeyed, clique em e clique em **discos de rechavear**.

Gerencie a criptografia com a CLI

Visão geral da criptografia NetApp

A NetApp oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

- A criptografia baseada em software usando o NetApp volume Encryption (NVE) é compatível com a criptografia de dados, um volume de cada vez
- A criptografia baseada em hardware usando o NetApp Storage Encryption (NSE) oferece suporte à criptografia de disco total (FDE) dos dados conforme são gravados.

Configurar a encriptação de volume NetApp

Configurar a visão geral da encriptação de volume do NetApp

O NetApp volume Encryption (NVE) é uma tecnologia baseada em software para criptografar dados em repouso, um volume de cada vez. Uma chave de criptografia acessível somente ao sistema de storage garante que os dados de volume não possam ser lidos se o dispositivo subjacente for reutilizado, retornado, extraviado ou roubado.

Compreender o NVE

Com o NVE, os metadados e os dados (incluindo cópias Snapshot) são criptografados. O acesso aos dados é dado por uma chave exclusiva XTS-AES-256, uma por volume. Um servidor de gerenciamento de chaves externo ou OKM (Onboard Key Manager) serve chaves para nós:

- O servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que serve chaves para nós que usam o Key Management Interoperability Protocol (KMIP). É uma prática recomendada configurar servidores de gerenciamento de chaves externos em um sistema de armazenamento diferente dos seus dados.
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves para nós do mesmo sistema de storage que seus dados.

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo. A licença VE está incluída no "ONTAP One". Sempre que um gerenciador de chaves externo ou integrado é configurado, há uma alteração na forma como a criptografia de dados em repouso é configurada para agregados novos e volumes novos. Agregados novos terão a encriptação agregada NetApp (NAE) ativada por predefinição. Volumes novos que não fazem parte de um agregado NAE terão a criptografia de volume NetApp (NVE) ativada por padrão. Se uma máquina virtual de storage de dados (SVM) for configurada com seu próprio gerenciador de

chaves usando o gerenciamento de chaves multilocatário, o volume criado para esse SVM será configurado automaticamente com NVE.

Pode ativar a encriptação num volume novo ou existente. O NVE dá suporte a uma variedade completa de recursos de eficiência de storage, incluindo deduplicação e compactação. Começando com ONTAP 9.14,1, você pode Habilite o NVE em volumes raiz do SVM atual.

> Se estiver usando o SnapLock, você poderá habilitar a criptografia somente em volumes SnapLock novos e vazios. Não é possível ativar a encriptação num volume SnapLock existente.

Você pode usar o NVE em qualquer tipo de agregado (HDD, SSD, híbrido, LUN de array), com qualquer tipo de RAID e em qualquer implementação de ONTAP com suporte, incluindo ONTAP Select. Você também pode usar o NVE com criptografia baseada em hardware para "criptografar dados" em unidades com autocriptografia.

Quando o NVE está ativado, o despejo de memória também é criptografado.

Criptografia em nível de agregado

Normalmente, cada volume criptografado recebe uma chave exclusiva. Quando o volume é excluído, a chave é excluída com ele.

A partir do ONTAP 9.6, você pode usar *NetApp Aggregate Encryption (NAE)* para atribuir chaves ao agregado que contém para que os volumes sejam criptografados. Quando um volume criptografado é excluído, as chaves do agregado são preservadas. As chaves são excluídas se todo o agregado for excluído.

Você deve usar criptografia em nível de agregado se planeja executar deduplicação in-line ou em segundo plano. De outra forma, a deduplicação em nível de agregado não é compatível com NVE.

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo.

Os volumes NVE e NAE podem coexistir no mesmo agregado. Os volumes encriptados em encriptação de nível agregado são volumes NAE por predefinição. Você pode substituir o padrão quando criptografar o volume.

Você pode usar o `volume move` comando para converter um volume NVE em um volume NAE e vice-versa. É possível replicar um volume NAE para um volume NVE.

Você não pode usar `secure purge` comandos em um volume NAE.

Quando usar servidores de gerenciamento de chaves externos

Embora seja menos caro e normalmente mais conveniente usar o gerenciador de chaves integrado, você deve configurar servidores KMIP se alguma das seguintes situações for verdadeira:

- Sua solução de gerenciamento de chaves de criptografia precisa estar em conformidade com Federal Information Processing Standards (FIPS) 140-2 ou com o padrão OASIS KMIP.
- Você precisa de uma solução de vários clusters, com gerenciamento centralizado de chaves de criptografia.
- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

Escopo do gerenciamento de chaves externas

O escopo do gerenciamento de chaves externas determina se os servidores de gerenciamento de chaves protegem todos os SVMs no cluster ou somente SVMs selecionadas:

- Você pode usar um *cluster scope* para configurar o gerenciamento de chaves externas para todos os SVMs no cluster. O administrador do cluster tem acesso a todas as chaves armazenadas nos servidores.
- A partir do ONTAP 9.6, você pode usar um *escopo SVM* para configurar o gerenciamento de chaves externas para um SVM nomeado no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para fornecer dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário.
- A partir do ONTAP 9.10,1, você pode usar o Azure Key Vault e Google Cloud KMS para proteger chaves NVE somente para SVMs de dados. Isso está disponível para o KMS da AWS a partir de 9.12.0.

Você pode usar ambos os escopos no mesmo cluster. Se os servidores de gerenciamento de chaves tiverem sido configurados para um SVM, o ONTAP usará apenas esses servidores para proteger chaves. Caso contrário, o ONTAP protege as chaves com os servidores de gerenciamento de chaves configurados para o cluster.

Uma lista de gerenciadores de chaves externos validados está disponível no "Ferramenta de Matriz de interoperabilidade NetApp (IMT)". Você pode encontrar esta lista inserindo o termo "key managers" no recurso de pesquisa do IMT.

Detalhes do suporte

A tabela a seguir mostra os detalhes de suporte do NVE:

Recurso ou recurso	Detalhes do suporte
Plataformas	Capacidade de descarga AES-NI necessária. Consulte o Hardware Universe (HWU) para verificar se o NVE e o NAE são compatíveis com sua plataforma.

Criptografia	A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você adiciona uma licença de criptografia de volume (VE) e tem um gerenciador de chaves integrado ou externo configurado. Se você precisar criar um agregado não criptografado, use o seguinte comando:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Se você precisar criar um volume de texto simples, use o seguinte comando:
	
	`volume create -encrypt false`
	
	A encriptação não está ativada por predefinição quando:
	
	• A licença VE não está instalada.
	• O gerenciador de chaves não está configurado.
	• Plataforma ou software não suporta criptografia.
	• A criptografia de hardware está ativada.

ONTAP	Todas as implementações do ONTAP. O suporte para ONTAP Cloud está disponível no ONTAP 9.5 e posterior.
Dispositivos	HDD, SSD, híbrido, array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Volumes de dados e volumes raiz atuais do SVM. Não é possível criptografar dados em volumes de metadados do MetroCluster. Em versões do ONTAP anteriores a 9.14.1, não é possível criptografar dados no volume raiz da SVM com NVE. A partir do ONTAP 9.14,1, o ONTAP suporta NVE em volumes raiz do SVM.
Criptografia em nível de agregado	A partir do ONTAP 9.6, o NVE é compatível com criptografia no nível de agregado (NAE): • Você deve usar criptografia em nível de agregado se planeja executar deduplicação in-line ou em segundo plano. • Você não pode rechavear um volume de criptografia de nível agregado. • A limpeza segura não é suportada em volumes de criptografia no nível de agregado. • Além dos volumes de dados, o NAE é compatível com a criptografia dos volumes raiz da SVM e do volume de metadados do MetroCluster. O NAE não suporta criptografia do volume raiz.
Escopo da SVM	A partir do ONTAP 9.6, o NVE é compatível com o escopo SVM somente para gerenciamento de chaves externas, e não para Gerenciador de chaves integrado. O MetroCluster é suportado a partir do ONTAP 9.8.
Eficiência de storage	Deduplicação, compressão, compactação, FlexClone. Os clones usam a mesma chave que o pai, mesmo depois de dividir o clone do pai. Você deve executar um `volume move` em um clone dividido, após o qual o clone dividido terá uma chave diferente.

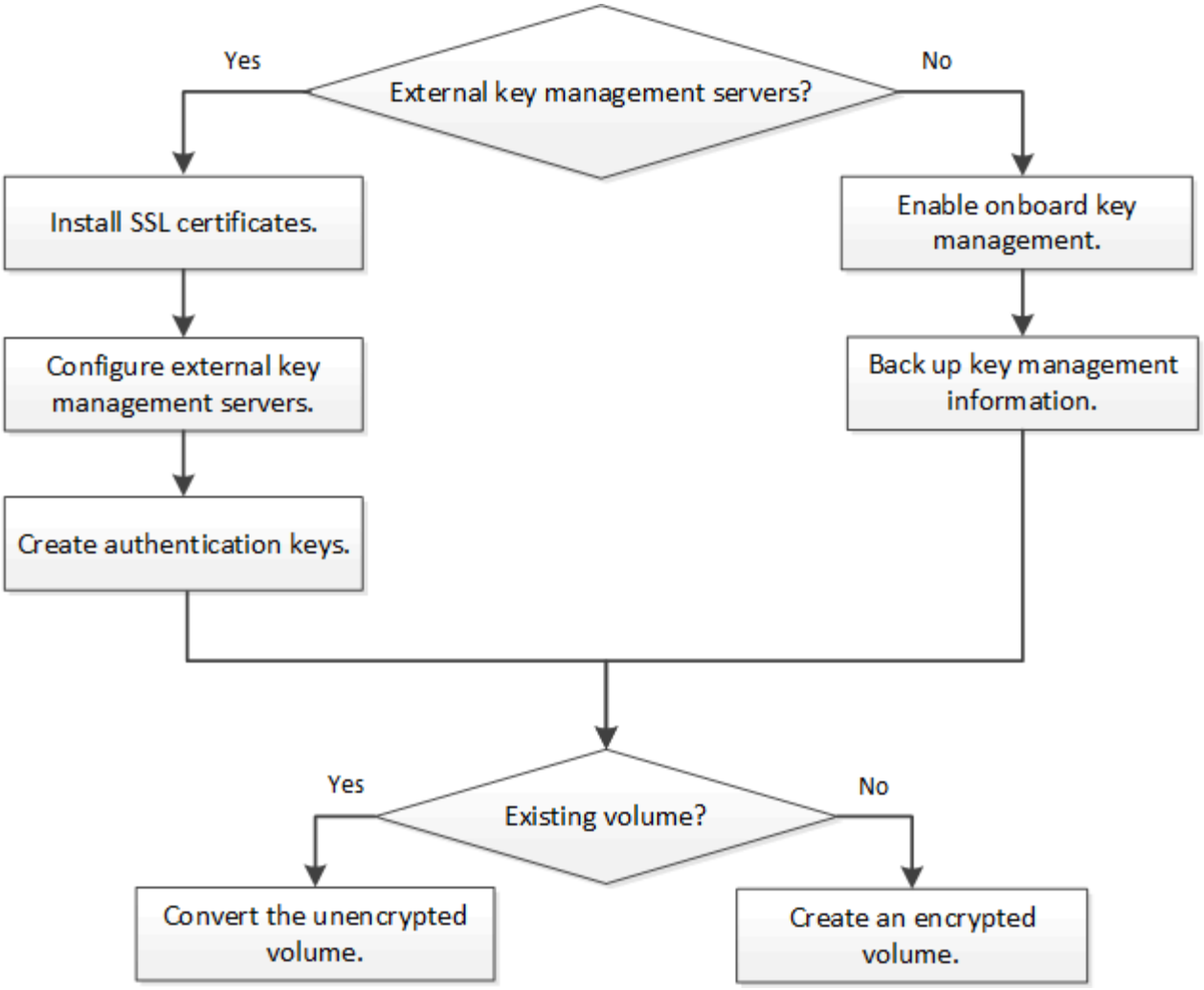
Replicação	• Para replicação de volume, os volumes de origem e destino podem ter configurações de criptografia diferentes. A criptografia pode ser configurada para a origem e não configurada para o destino e vice-versa. A encriptação configurada na origem não será replicada para o destino. A criptografia deve ser configurada manualmente na origem e no destino. Configurar o NVEConsulte e Criptografia de dados de volume com NVE. • Para a replicação SVM, o volume de destino é criptografado automaticamente, a menos que o destino não contenha um nó compatível com criptografia de volume. Nesse caso, a replicação seja bem-sucedida, mas o volume de destino não seja criptografado. • Para configurações do MetroCluster, cada cluster puxa chaves de gerenciamento de chaves externas de seus servidores de chaves configurados. As chaves OKM são replicadas para o site do parceiro pelo serviço de replicação de configuração.
Conformidade	A partir do ONTAP 9.2, o SnapLock tem suporte nos modos conformidade e empresa, apenas para novos volumes. Não é possível ativar a encriptação num volume SnapLock existente.
FlexGroups	A partir do ONTAP 9.2, os grupos flexíveis são suportados. Os agregados de destino devem ser do mesmo tipo que os agregados de origem, tanto em nível de volume como em nível de agregado. A partir do ONTAP 9.5, é suportada a rechavear no local de volumes FlexGroup.
Transição de 7 modos	A partir da ferramenta de transição de 7 modos 3,3, você pode usar a CLI da ferramenta de transição de 7 modos para realizar a transição baseada em cópia para volumes de destino habilitados para NVE no sistema em cluster.

Informações relacionadas

"Perguntas frequentes - encriptação de volume NetApp e encriptação agregada NetApp"

Fluxo de trabalho do NetApp volume Encryption

Você deve configurar os serviços de gerenciamento de chaves antes de ativar a criptografia de volume. Pode ativar a encriptação num novo volume ou num volume existente.



"Tem de instalar a licença VE" E configure os serviços de gerenciamento de chaves antes de criptografar dados com NVE. Antes de instalar a licença, você deve "Determine se sua versão do ONTAP é compatível com NVE".

Configurar o NVE

Determine se a versão do cluster é compatível com NVE

Você deve determinar se a versão do cluster é compatível com NVE antes de instalar a licença. Você pode usar o `version` comando para determinar a versão do cluster.

Sobre esta tarefa

A versão do cluster é a versão mais baixa do ONTAP em execução em qualquer nó no cluster.

Passo

1. Determine se a versão do cluster é compatível com NVE:

   ```
   version -v
   ```

   NVE não é suportado se o comando output exibir o texto "'1Ono-DARE" (para "'criptografia sem dados em repouso"') ou se você estiver usando uma plataforma que não está listada no "Detalhes do suporte".

O comando a seguir determina se o NVE é suportado `cluster1` no .

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

A saída de `1Ono-DARE` indica que o NVE não é suportado na versão do cluster.

Instale a licença

Uma licença VE permite que você use o recurso em todos os nós do cluster. Essa licença é necessária para que você possa criptografar dados com NVE. Está incluído com "ONTAP One".

Antes do ONTAP One, a licença VE foi incluída com o pacote de encriptação. O pacote de criptografia não é mais oferecido, mas ainda é válido. Embora não seja necessário atualmente, os clientes existentes podem optar por "Atualize para o ONTAP One".

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Tem de ter recebido a chave de licença VE do seu representante de vendas ou ter o ONTAP One instalado.

Passos

1. "Verifique se a licença VE está instalada".

   O nome do pacote de licença VE é `VE`.

2. Se a licença não estiver instalada, "Use o Gerenciador do sistema ou a CLI do ONTAP para instalá-lo".

Configurar o gerenciamento de chaves externas

Configurar uma visão geral do gerenciamento de chaves externas

Você pode usar um ou mais servidores de gerenciamento de chaves externos para proteger as chaves que o cluster usa para acessar dados criptografados. Um servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que serve chaves para nós que usam o Key Management Interoperability Protocol (KMIP).

> Para o ONTAP 9.1 e versões anteriores, as LIFs de gerenciamento de nós devem ser atribuídas a portas configuradas com a função de gerenciamento de nó antes de usar o gerenciador de chaves externo.

O NetApp volume Encryption (NVE) é compatível com o Gerenciador de chaves integrado no ONTAP 9.1 e posterior. A partir do ONTAP 9.3, o NVE é compatível com gerenciamento de chaves externas (KMIP) e Gerenciador de chaves integrado. A partir do ONTAP 9.10,1, você pode usar Serviço do Azure Key Vault ou do Google Cloud Key Manager para proteger suas chaves NVE. A partir do ONTAP 9.11,1, você pode configurar vários gerenciadores de chaves externos em um cluster. Consulte Configurar servidores de chaves em cluster.

Gerencie gerenciadores de chaves externos com o System Manager

A partir do ONTAP 9.7, você pode armazenar e gerenciar chaves de autenticação e criptografia com o Gerenciador de chaves integrado. A partir do ONTAP 9.13,1, você também pode usar gerenciadores de chaves externos para armazenar e gerenciar essas chaves.

O Gerenciador de chaves integrado armazena e gerencia chaves em um banco de dados seguro interno ao cluster. Seu escopo é o cluster. Um gerenciador de chaves externo armazena e gerencia chaves fora do cluster. Seu escopo pode ser o cluster ou a VM de storage. Um ou mais gerenciadores de chaves externos podem ser usados. Aplicam-se as seguintes condições:

- Se o Gerenciador de chaves integrado estiver habilitado, um gerenciador de chaves externo não poderá ser habilitado no nível do cluster, mas poderá ser habilitado no nível da VM de armazenamento.
- Se um gerenciador de chaves externo estiver habilitado no nível do cluster, o Gerenciador de chaves integrado não poderá ser habilitado.

Ao usar gerenciadores de chaves externos, você pode Registrar até quatro servidores de chaves primárias por VM de armazenamento e cluster. Cada servidor de chave primária pode ser agrupado com até três servidores de chaves secundárias.

Configurar um gerenciador de chaves externo

Para adicionar um gerenciador de chaves externo para uma VM de armazenamento, você deve adicionar um gateway opcional ao configurar a interface de rede para a VM de armazenamento. Se a VM de armazenamento foi criada sem a rota de rede, você terá que criar a rota explicitamente para o gerenciador de chaves externo. "Criar um LIF (interface de rede)"Consulte .

Passos

Você pode configurar um gerenciador de chaves externo a partir de diferentes locais no System Manager.

1. Para configurar um gerenciador de chaves externo, execute um dos seguintes passos iniciais.

Fluxo de trabalho	Navegação	Etapa inicial
Configure o Gerenciador de chaves	**Cluster** > **Settings**	Role até a seção **Segurança**. Em **encriptação**, selecione . Selecione **External Key Manager**.
Adicionar nível local	**Armazenamento** > **camadas**	Selecione * Adicionar nível local*. Marque a caixa de seleção "Configurar Gerenciador de chaves". Selecione **External Key Manager**.
Prepare o armazenamento	**Painel**	Na seção **capacidade**, selecione **preparar armazenamento**. Em seguida, selecione "Configure Key Manager". Selecione **External Key Manager**.
Configurar a criptografia (gerenciador de chaves somente no escopo da VM de storage)	**Storage** > **Storage VMs**	Selecione a VM de armazenamento. Selecione a guia **Configurações**. Na seção **criptografia** em **Segurança**, selecione .

2. Para adicionar um servidor de chave primária, selecione + Add e preencha os campos **Endereço IP ou Nome do host** e **porta**.
3. Os certificados instalados existentes são listados nos campos **certificados KMIP Server CA** e **KMIP Client Certificate**. Você pode executar qualquer uma das seguintes ações:
   - Selecione para selecionar os certificados instalados que pretende mapear para o gestor de chaves. (Podem ser selecionados vários certificados de CA de serviço, mas apenas um certificado de cliente pode ser selecionado.)
   - Selecione **Adicionar novo certificado** para adicionar um certificado que ainda não tenha sido instalado e mapeie-o para o gerenciador de chaves externo.
   - Selecione ao lado do nome do certificado para excluir os certificados instalados que você não deseja mapear para o gerenciador de chaves externo.
4. Para adicionar um servidor de chaves secundário, selecione **Add** na coluna **Secondary Key Servers** e forneça seus detalhes.
5. Selecione **Save** para concluir a configuração.

Editar um gerenciador de chaves externo existente

Se você já tiver configurado um gerenciador de chaves externo, poderá modificar suas configurações.

Passos

1. Para editar a configuração de um gerenciador de chaves externo, execute um dos seguintes passos iniciais.

Âmbito de aplicação	Navegação	Etapa inicial
Gerenciador de chaves externo do escopo do cluster	**Cluster** > **Settings**	Role até a seção **Segurança**. Em **Encryption**, selecione e, em seguida, selecione **Edit External Key Manager**.
Gerenciador de chaves externo de escopo da VM de storage	**Storage** > **Storage VMs**	Selecione a VM de armazenamento. Selecione a guia **Configurações**. Na seção **criptografia** em **Segurança**, selecione e selecione **Editar Gerenciador de chaves externas**.

2. Os servidores de chave existentes estão listados na tabela **Key Servers**. Você pode executar as seguintes operações:
   - Adicione um novo servidor de chaves selecionando + Add .
   - Exclua um servidor de chaves selecionando no final da célula da tabela que contém o nome do servidor de chaves. Os servidores de chave secundária associados a esse servidor de chave primária também são removidos da configuração.

Excluir um gerenciador de chaves externo

Um gerenciador de chaves externo pode ser excluído se os volumes não forem criptografados.

Passos

1. Para excluir um gerenciador de chaves externo, execute uma das etapas a seguir.

Âmbito de aplicação	Navegação	Etapa inicial
Gerenciador de chaves externo do escopo do cluster	**Cluster** > **Settings**	Role até a seção **Segurança**. Em **Encryption**, selecione e, em seguida, selecione **Delete External Key Manager**.
Gerenciador de chaves externo de escopo da VM de storage	**Storage** > **Storage VMs**	Selecione a VM de armazenamento. Selecione a guia **Configurações**. Na seção **criptografia** em **Segurança**, selecione e selecione **Excluir Gerenciador de chaves externas**.

Instale certificados SSL no cluster

O cluster e o servidor KMIP usam certificados SSL KMIP para verificar a identidade uns dos outros e estabelecer uma conexão SSL. Antes de configurar a conexão SSL com o servidor KMIP, você deve instalar os certificados SSL do cliente KMIP para o cluster e o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.

Sobre esta tarefa

Em um par de HA, ambos os nós precisam usar os mesmos certificados KMIP SSL públicos e privados. Se você conectar vários pares de HA ao mesmo servidor KMIP, todos os nós dos pares de HA precisarão usar os mesmos certificados KMIP SSL públicos e privados.

Antes de começar

- O tempo deve ser sincronizado no servidor criando os certificados, o servidor KMIP e o cluster.
- Você deve ter obtido o certificado de cliente KMIP SSL público para o cluster.
- Você deve ter obtido a chave privada associada ao certificado de cliente SSL KMIP para o cluster.
- O certificado de cliente SSL KMIP não deve ser protegido por senha.
- Você deve ter obtido o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.
- Em um ambiente MetroCluster, é necessário instalar os mesmos certificados SSL KMIP em ambos os clusters.

> Você pode instalar os certificados de cliente e servidor no servidor KMIP antes ou depois de instalar os certificados no cluster.

Passos

1. Instale os certificados de cliente SSL KMIP para o cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Você será solicitado a inserir os certificados SSL KMIP público e privado.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Instale o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

Habilite o gerenciamento de chaves externas no ONTAP 9.6 e versões posteriores (NVE)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. A partir do ONTAP 9.6, você tem a opção de configurar um gerenciador de chaves externo separado para proteger as chaves que um SVM de dados usa para acessar dados criptografados.

A partir do ONTAP 9.11,1, você pode adicionar até 3 servidores de chaves secundárias por servidor de chaves primárias para criar um servidor de chaves em cluster. Para obter mais informações, Configurar servidores de chaves externas em clusterconsulte .

Sobre esta tarefa

É possível conectar até quatro servidores KMIP a um cluster ou SVM. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

O escopo do gerenciamento de chaves externas determina se os servidores de gerenciamento de chaves protegem todos os SVMs no cluster ou somente SVMs selecionadas:

- Você pode usar um *cluster scope* para configurar o gerenciamento de chaves externas para todos os SVMs no cluster. O administrador do cluster tem acesso a todas as chaves armazenadas nos servidores.
- A partir do ONTAP 9.6, você pode usar um *escopo SVM* para configurar o gerenciamento de chaves externas para um SVM de dados no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para fornecer dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário.
- Para ambientes multitenant, instale uma licença para *MT_EK_MGMT* usando o seguinte comando:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Para obter a sintaxe de comando completa, consulte a página man para o comando.

Você pode usar ambos os escopos no mesmo cluster. Se os servidores de gerenciamento de chaves tiverem sido configurados para um SVM, o ONTAP usará apenas esses servidores para proteger chaves. Caso contrário, o ONTAP protege as chaves com os servidores de gerenciamento de chaves configurados para o cluster.

Você pode configurar o gerenciamento de chaves integradas no escopo do cluster e o gerenciamento de chaves externas no escopo da SVM. Você pode usar o `security key-manager key migrate` comando para migrar chaves do gerenciamento de chaves integradas no escopo do cluster para gerenciadores de chaves externos no escopo da SVM.

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Para habilitar o gerenciamento de chaves externas para um ambiente MetroCluster, o MetroCluster deve estar totalmente configurado antes de habilitar o gerenciamento de chaves externas.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

Passos

1. Configurar a conetividade do gerenciador de chaves para o cluster:

   `security key-manager external enable -vserver admin_SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   - O `security key-manager external enable` comando substitui o `security key-manager setup` comando. Se você executar o comando no prompt de login do cluster, *`admin_SVM`* o padrão será o administrador SVM do cluster atual. Você deve ser o administrador do cluster para configurar o escopo do cluster. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.
   - Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para o SVM de administrador, repita o `security key-manager external enable` comando no cluster de parceiros.

   O comando a seguir habilita o gerenciamento de chaves externas para `cluster1` com três servidores de chaves externas. O primeiro servidor de chaves é especificado usando seu nome de host e porta, o segundo é especificado usando um endereço IP e a porta padrão, e o terceiro é especificado usando um endereço IPv6 e porta:

   ```
   clusterl::> security key-manager external enable -vserver cluster1 -key
   -servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Configurar um gerenciador de chaves e uma SVM:

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   - Se você executar o comando no prompt de login SVM, `SVM` o padrão será SVM atual. Você precisa ser um administrador de cluster ou SVM para configurar o escopo do SVM. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.
   - Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para um SVM de dados, não será necessário repetir o `security key-manager external enable` comando no cluster de parceiros.

   O comando a seguir habilita o gerenciamento de chaves externas para `svm1` que um servidor de chave única esteja escutando na porta padrão 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repita a última etapa para quaisquer SVMs adicionais.

> Você também pode usar o `security key-manager external add-servers` comando para configurar SVMs adicionais. O `security key-manager external add-servers` comando substitui o `security key-manager add` comando. Para obter a sintaxe completa do comando, consulte a página man.

4. Verifique se todos os servidores KMIP configurados estão conetados:

`security key-manager external show-status -node node_name`

> O `security key-manager external show-status` comando substitui o `security key-manager show -status` comando. Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. Opcionalmente, converta volumes de texto simples em volumes criptografados.

`volume encryption conversion start`

Um gerenciador de chaves externo deve estar totalmente configurado antes de converter os volumes. Em

um ambiente MetroCluster, um gerenciador de chaves externo deve ser configurado em ambos os locais.

Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. É possível conectar até quatro servidores KMIP a um nó. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

Sobre esta tarefa

O ONTAP configura a conectividade do servidor KMIP para todos os nós no cluster.

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

Passos

1. Configurar a conectividade do gerenciador de chaves para nós de cluster:

   ```
   security key-manager setup
   ```

   A configuração do gerenciador de chaves é iniciada.

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

2. Insira a resposta apropriada em cada prompt.
3. Adicionar um servidor KMIP:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

4. Adicione um servidor KMIP adicional para redundância:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

5. Verifique se todos os servidores KMIP configurados estão conetados:

   ```
   security key-manager show -status
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. Opcionalmente, converta volumes de texto simples em volumes criptografados.

   ```
   volume encryption conversion start
   ```

   Um gerenciador de chaves externo deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, um gerenciador de chaves externo deve ser configurado em ambos os locais.

Gerencie chaves com um provedor de nuvem

A partir do ONTAP 9.10,1, você pode usar "Azure Key Vault (AKV)" e "Serviço de gerenciamento de chaves do Google Cloud Platform (Cloud KMS)"proteger suas chaves de criptografia ONTAP em um aplicativo hospedado na nuvem. A partir do ONTAP 9.12,0, também é possível proteger as chaves NVE com "KMS DA AWS"o .

O AWS KMS, AKV e o Cloud KMS podem ser usados para proteger "Chaves de criptografia de volume NetApp (NVE)" somente SVMs de dados.

Sobre esta tarefa

O gerenciamento de chaves com um fornecedor de nuvem pode ser habilitado com a CLI ou a API REST do ONTAP.

Ao usar um provedor de nuvem para proteger suas chaves, esteja ciente de que, por padrão, um data SVM LIF é usado para se comunicar com o endpoint de gerenciamento de chaves na nuvem. Uma rede de gerenciamento de nós é usada para se comunicar com os serviços de autenticação do provedor de nuvem (login.microsoftonline.com para Azure; oauth2.googleapis.com para Cloud KMS). Se a rede do cluster não estiver configurada corretamente, o cluster não utilizará adequadamente o serviço de gerenciamento de chaves.

Ao utilizar um serviço de gerenciamento de chaves do provedor de nuvem, você deve estar ciente das seguintes limitações:

- O gerenciamento de chaves do fornecedor de nuvem não está disponível para criptografia de storage NetApp (NSE) e criptografia agregada NetApp (NAE). "KMIPs externos" pode ser usado em vez disso.
- O gerenciamento de chaves do fornecedor de nuvem não está disponível para configurações do MetroCluster.

- O gerenciamento de chaves do fornecedor de nuvem só pode ser configurado em um data SVM.

Antes de começar

- Você deve ter configurado o KMS no provedor de nuvem apropriado.
- Os nós do cluster do ONTAP devem ser compatíveis com NVE.
- "Você deve ter instalado as licenças de criptografia de volume (VE) e gerenciamento de chaves de criptografia de vários locatários (MTEKM)". Estas licenças estão incluídas no "ONTAP One".
- Você precisa ser um administrador de cluster ou SVM.
- O SVM não deve incluir volumes criptografados nem empregar um gerenciador de chaves. Se o SVM de dados incluir volumes criptografados, você precisará migrá-los antes de configurar o KMS.

Ativar o gerenciamento de chaves externas

A ativação do gerenciamento de chaves externas depende do gerenciador de chaves específico que você usa. Escolha a guia do gerenciador de chaves e do ambiente apropriados.

AWS

Antes de começar

- Você deve criar uma subvenção para a chave AWS KMS que será usada pela função de gerenciamento de criptografia do IAM. A função IAM deve incluir uma política que permita as seguintes operações:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt` Para obter mais informações, consulte a documentação da AWS para "subvenções".

Habilite o AWS KMV em um SVM do ONTAP

1. Antes de começar, obtenha o ID da chave de acesso e a chave secreta do seu AWS KMS.
2. Defina o nível de privilégio como avançado:
   `set -priv advanced`
3. Habilite o AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando solicitado, insira a chave secreta.
5. Confirme se o AWS KMS foi configurado corretamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Habilite o cofre de chaves do Azure em um SVM do ONTAP

1. Antes de começar, você precisa obter as credenciais de autenticação apropriadas da sua conta Azure, seja um segredo de cliente ou certificado. Você também precisa garantir que todos os nós no cluster estejam íntegros. Você pode verificar isso com o comando `cluster show`.
2. Defina o nível privilegiado como avançado
   `set -priv advanced`
3. Ativar AKV no SVM
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}` quando solicitado, insira o certificado de cliente ou o segredo do cliente na sua conta Azure.
4. Verifique se o AKV está ativado corretamente:
   `security key-manager external azure show vserver` *`svm_name`* Se a acessibilidade do serviço não estiver OK, estabeleça a conetividade com o serviço de gerenciamento de chaves AKV através dos dados SVM LIF.

Google Cloud

Habilite o KMS da nuvem em um SVM do ONTAP

1. Antes de começar, obtenha a chave privada para o arquivo de chave de conta KMS do Google Cloud em um formato JSON. Isso pode ser encontrado na sua conta do GCP. Você também precisa garantir que todos os nós no cluster estejam íntegros. Você pode verificar isso com o comando `cluster show`.
2. Defina o nível privilegiado como avançado:
   `set -priv advanced`

3. Ative o Cloud KMS no SVM
`security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`* quando solicitado, insira o conteúdo do arquivo JSON com a chave privada da conta de serviço
4. Verifique se o Cloud KMS está configurado com os parâmetros corretos:
`security key-manager external gcp show vserver` *`svm_name`* O status do `kms_wrapped_key_status` será "`UNKNOWN`" se nenhum volume criptografado tiver sido criado. Se a acessibilidade do serviço não estiver OK, estabeleça a conectividade com o serviço de gerenciamento de chaves do GCP por meio do data SVM LIF.

Se um ou mais volumes criptografados já estiverem configurados para um SVM de dados e as chaves NVE correspondentes forem gerenciadas pelo gerenciador de chaves integrado SVM de administrador, essas chaves deverão ser migradas para o serviço de gerenciamento de chaves externo. Para fazer isso com a CLI, execute o comando:
`security key-manager key migrate -from-Vserver` *`admin_SVM`* `-to-Vserver` *`data_SVM`*
Novos volumes criptografados não podem ser criados para o SVM de dados do locatário até que todas as chaves NVE do SVM de dados sejam migradas com sucesso.

Informações relacionadas

- "Criptografia de volumes com soluções de criptografia NetApp para Cloud Volumes ONTAP"

Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior (NVE)

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário ativar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager onboard sync` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, deverá executar primeiro o `security key-manager onboard enable` comando no cluster local e, em seguida, executar o `security key-manager onboard sync` comando no cluster remoto, usando a mesma senha em cada um. Ao executar o `security key-manager onboard enable` comando a partir do cluster local e depois sincronizar no cluster remoto, não é necessário executar o `enable` comando novamente a partir do cluster remoto.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. Pode utilizar a `cc-mode-enabled=yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `cc-mode-enabled=yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Ao configurar a criptografia de dados em repouso do ONTAP, para atender aos requisitos de soluções comerciais para classificação (CSfC), você deve usar o NSE com NVE e garantir que o Gerenciador de chaves integrado esteja habilitado no modo critérios comuns. Consulte a "Resumo da solução CSfC"para

obter mais informações sobre o CSfC.

Quando o Gerenciador de chaves integrado está habilitado no modo Common Criteria (`cc-mode-enabled=yes`), o comportamento do sistema é alterado das seguintes maneiras:

- O sistema monitoriza as tentativas consecutivas de frase-passe do cluster falhadas ao funcionar no modo Common Criteria (critérios comuns).

  Se não conseguir introduzir a frase-passe correta do cluster no arranque, os volumes encriptados não são montados. Para corrigir isso, você deve reinicializar o nó e inserir a senha correta do cluster. Uma vez iniciado, o sistema permite até 5 tentativas consecutivas para inserir corretamente a senha do cluster em um período de 24 horas para qualquer comando que exija a senha do cluster como um parâmetro. Se o limite for atingido (por exemplo, você não conseguiu inserir corretamente a senha do cluster 5 vezes em uma linha), então você deve esperar o período de tempo limite de 24 horas para decorrer, ou você deve reiniciar o nó, a fim de redefinir o limite.

- As atualizações de imagem do sistema usam o certificado de assinatura de código NetApp RSA-3072 juntamente com os digests assinados por código SHA-384 para verificar a integridade da imagem em vez do certificado de assinatura de código NetApp RSA-2048 usual e os digests assinados por código SHA-256.

  O comando upgrade verifica se o conteúdo da imagem não foi alterado ou corrompido verificando várias assinaturas digitais. O processo de atualização da imagem prossegue para o próximo passo se a validação for bem-sucedida; caso contrário, a atualização da imagem falhará. Consulte a `cluster image` página de manual para obter informações sobre atualizações do sistema.

O Gerenciador de chaves integrado armazena as chaves na memória volátil. O conteúdo da memória volátil é apagado quando o sistema é reinicializado ou interrompido. Em condições normais de funcionamento, o conteúdo da memória volátil será apagado dentro de 30sMB quando um sistema for interrompido.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar o Gerenciador de chaves integrado.

Passos

1. Inicie a configuração do gerenciador de chaves:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

Defina `cc-mode-enabled=yes` para exigir que os usuários inseram a senha do gerenciador de chaves após uma reinicialização. Para NVE, se você definir `cc-mode-enabled=yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. A – `cc-mode-enabled` opção não é suportada nas configurações do MetroCluster. O `security key-manager onboard enable` comando substitui o `security key-manager setup` comando.

O exemplo a seguir inicia o comando de configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

3. No prompt de confirmação da senha, redigite a senha.
4. Verifique se as chaves de autenticação foram criadas:

```
security key-manager key query -key-type NSE-AK
```

> O `security key-manager key query` comando substitui o `security key-manager query key` comando. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                  Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Opcionalmente, converta volumes de texto simples em volumes criptografados.

   `volume encryption conversion start`

   O Gerenciador de chaves integrado deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, o Gerenciador de chaves integrado deve ser configurado em ambos os sites.

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "Faça backup manual das informações de gerenciamento de chaves integradas"Consulte .

Habilite o gerenciamento de chaves integradas no ONTAP 9.5 e versões anteriores (NVE)

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Antes de começar

- Se você estiver usando o NSE ou o NVE com um servidor de gerenciamento de chaves externo (KMIP), exclua o banco de dados do gerenciador de chaves externo.

  "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar o Gerenciador de chaves integrado.

Passos

1. Inicie a configuração do gerenciador de chaves:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe do gestor de chaves após uma reinicialização. Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente.

   O exemplo a seguir inicia a configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Digite `yes` no prompt para configurar o gerenciamento de chaves integradas.
3. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

4. No prompt de confirmação da senha, redigite a senha.
5. Verifique se as chaves estão configuradas para todos os nós:

   `security key-manager key show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Opcionalmente, converta volumes de texto simples em volumes criptografados.

   `volume encryption conversion start`

   O Gerenciador de chaves integrado deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, o Gerenciador de chaves integrado deve ser configurado em ambos os sites.

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "Faça backup manual das informações de gerenciamento de chaves integradas"Consulte .

Habilite o gerenciamento de chaves integradas em nós recém-adicionados

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

> Para o ONTAP 9.5 e versões anteriores, você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.
>
> Para o ONTAP 9.6 e posterior, você deve executar o `security key-manager sync` comando sempre que adicionar um nó ao cluster.
>
> Se você adicionar um nó a um cluster que tenha o gerenciamento de chaves integradas configurado, você executará esse comando para atualizar as chaves ausentes.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- A partir do ONTAP 9.6, é necessário executar `security key-manager onboard enable` primeiro no cluster local e, em seguida, executar `security key-manager onboard sync` no cluster remoto, usando a mesma frase-passe em cada um.
- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Migrar chaves de criptografia de dados do ONTAP entre gerenciadores de chaves

Você pode gerenciar suas chaves de criptografia de dados usando o Gerenciador de chaves integrado do ONTAP ou um gerenciador de chaves externo (ou ambos). Os gerenciadores de chaves externos só podem ser ativados no nível de VM de armazenamento. No nível do cluster do ONTAP, você pode ativar o gerenciador de chaves integrado ou um gerenciador de chaves externo.

Se ativar o seu gestor de chaves na…	Você pode usar…
Somente no nível do cluster	O gerenciador de chaves integrado ou um gerenciador de chaves externo
Somente nível SVM	Apenas um gerenciador de chaves externo
Tanto o cluster quanto o nível da SVM	Uma das seguintes combinações de gerenciador de chaves: • Opção 1 Nível de cluster: Gerenciador de chaves integrado Nível da SVM: Gerente de chaves externo • Opção 2 Nível de cluster: Gerenciador de chaves externo Nível da SVM: Gerente de chaves externo

Migre chaves entre os gerenciadores-chave no nível do cluster do ONTAP

A partir do ONTAP 9.16,1, você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre gerenciadores de chaves no nível do cluster.

Do gerenciador de chaves integrado ao gerenciador de chaves externo

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração de gerenciador de chaves externo inativo:

```
security key-manager external create-config
```

3. Mude para o gerenciador de chaves externo:

```
security key-manager keystore enable -vserver <svm_name> -type KMIP
```

4. Exclua a configuração do gerenciador de chaves integrado:

```
security key-manager keystore delete-config -vserver <svm_name>
-type OKM
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Do gerenciador de chaves externo ao gerenciador de chaves integrado

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração inativa do gerenciador de chaves integrado:

```
security key-manager onboard create-config
```

3. Ative a configuração do gerenciador de chaves integrado:

```
security key-manager keystore enable -vserver <svm_name> -type OKM
```

4. Exclua a configuração do gerenciador de chaves externo

```
security key-manager keystore delete-config -vserver <svm_name>
-type KMIP
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Migre chaves entre gerenciadores de chaves em cluster ONTAP e níveis de VM de armazenamento

Você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre o gerenciador de chaves no nível do cluster e um gerenciador de chaves no nível da VM de storage.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Migrar as chaves:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<svm_name>
```

3. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Criptografia de dados de volume com NVE

Criptografe dados de volume com a visão geral do NVE

A partir do ONTAP 9.7, a criptografia de agregado e volume é ativada por padrão quando você tem a licença VE e o gerenciamento de chaves internas ou externas. Para o ONTAP 9.6 e versões anteriores, é possível ativar a criptografia em um novo volume ou em um volume existente. Tem de ter instalado a licença VE e ativado a gestão de chaves para poder ativar a encriptação de volume. O NVE está em conformidade com FIPS-140-2 nível 1.

Ative a encriptação em nível de agregado com licença VE

A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você tem o "Licença VE" e gerenciamento de chaves externas ou

integradas. A partir do ONTAP 9.6, você pode usar a criptografia em nível de agregado para atribuir chaves ao agregado que contém para que os volumes sejam criptografados.

Sobre esta tarefa

Você deve usar criptografia em nível de agregado se planeja executar deduplicação in-line ou em segundo plano. De outra forma, a deduplicação em nível de agregado não é compatível com NVE.

Um agregado habilitado para criptografia de nível agregado é chamado de *agregado NAE* (para criptografia agregada NetApp). Todos os volumes em um agregado NAE precisam ser criptografados com criptografia NAE ou NVE. Com a criptografia de nível agregado, os volumes criados no agregado são criptografados com criptografia NAE por padrão. Em vez disso, você pode substituir o padrão para usar a criptografia NVE.

Os volumes de texto sem formatação não são suportados em agregados NAE.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Ativar ou desativar a encriptação de nível agregado:

Para…	Use este comando…
Crie um agregado NAE com o ONTAP 9.7 ou posterior	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Crie um agregado NAE com o ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Converter um agregado não-naE em um agregado NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Converter um agregado NAE em um agregado não-naE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Para obter a sintaxe completa do comando, consulte as páginas man.

O comando a seguir habilita a criptografia de nível agregado `aggr1` no :

- ONTAP 9.7 ou posterior:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 ou anterior:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Verifique se o agregado está habilitado para criptografia:

   `storage aggregate show -fields encrypt-with-aggr-key`

   Para obter a sintaxe completa do comando, consulte a página man.

   O comando a seguir verifica se `aggr1` está habilitado para criptografia:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Depois de terminar

Execute o `volume create` comando para criar os volumes criptografados.

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP automaticamente "envia" uma chave de criptografia para o servidor quando você criptografa um volume.

Ative a criptografia em um novo volume

Você pode usar o `volume create` comando para habilitar a criptografia em um novo volume.

Sobre esta tarefa

É possível criptografar volumes usando o NetApp volume Encryption (NVE) e, a partir do ONTAP 9.6, NetApp Aggregate Encryption (NAE). Para saber mais sobre NAE e NVE, consulte o descrição geral da encriptação de volumes.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

O procedimento para habilitar a criptografia em um novo volume no ONTAP varia de acordo com a versão do ONTAP que você está usando e sua configuração específica:

- A partir do ONTAP 9.4, se você ativar `cc-mode` ao configurar o Gerenciador de chaves integrado, os volumes criados com o `volume create` comando serão automaticamente criptografados, independentemente de você especificar ou não `-encrypt true` .
- No ONTAP 9.6 e versões anteriores, você deve usar `-encrypt true` comandos com `volume create` para ativar a criptografia (desde que não tenha ativado `cc-mode`).
- Se você quiser criar um volume NAE no ONTAP 9.6, você deve habilitar o NAE no nível agregado. Ative a encriptação em nível de agregado com a licença VEConsulte para obter mais detalhes sobre esta tarefa.

- A partir do ONTAP 9.7, os volumes recém-criados são criptografados por padrão quando você tem o "Licença VE" e gerenciamento de chaves integradas ou externas. Por padrão, novos volumes criados em um agregado NAE serão do tipo NAE em vez de NVE.
  - No ONTAP 9.7 e versões posteriores, se você adicionar `-encrypt true` ao `volume create` comando para criar um volume em um agregado NAE, o volume terá criptografia NVE em vez de NAE. Todos os volumes em um agregado NAE precisam ser criptografados com NVE ou NAE.

Os volumes de texto sem formatação não são suportados em agregados NAE.

Passos

1. Crie um novo volume e especifique se a criptografia está ativada no volume. Se o novo volume estiver em um agregado NAE, por padrão o volume será um volume NAE:

Para criar…	Use este comando…
Um volume NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Um volume NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` E No ONTAP 9.6 e anterior, em que o NAE não é suportado, `-encrypt true` especifica que o volume deve ser criptografado com NVE. No ONTAP 9.7 e posterior, onde os volumes são criados em agregados NAE, `-encrypt true` substitui o tipo de criptografia padrão do NAE para criar um volume NVE.
Um volume de texto simples	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/volume-create.html[`volume create` em referência de comando ONTAP.

2. Verifique se os volumes estão ativados para criptografia:

   ```
   volume show -is-encrypted true
   ```

   Para obter a sintaxe de comando completa, consulte "Referência do comando ONTAP".

Resultado

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP "enviará" automaticamente uma chave de criptografia ao servidor quando você criptografar um volume.

=
:allow-uri-read:

Ative a criptografia em um volume existente

Você pode usar o `volume move start` comando ou o `volume encryption conversion start` para habilitar a criptografia em um volume existente.

Sobre esta tarefa

- A partir do ONTAP 9.3, você pode usar o `volume encryption conversion start` comando para habilitar a criptografia de um volume existente "no lugar", sem ter que mover o volume para um local diferente. Alternativamente, você pode usar o `volume move start` comando.
- Para o ONTAP 9.2 e versões anteriores, você pode usar apenas o `volume move start` comando para habilitar a criptografia movendo um volume existente.

Ative a criptografia em um volume existente com o comando de início da conversão de criptografia de volume

A partir do ONTAP 9.3, você pode usar o `volume encryption conversion start` comando para habilitar a criptografia de um volume existente "no lugar", sem ter que mover o volume para um local diferente.

Depois de iniciar uma operação de conversão, ela deve ser concluída. Se você encontrar um problema de desempenho durante a operação, você pode executar o `volume encryption conversion pause` comando para pausar a operação e o `volume encryption conversion resume` comando para retomar a operação.

> Não pode utilizar `volume encryption conversion start` para converter um volume SnapLock.

Passos

1. Ativar encriptação num volume existente:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   Para a sintaxe de comando inteira, consulte a página man para o comando.

   O comando a seguir habilita a criptografia no volume `vol1`existente :

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   O sistema cria uma chave de criptografia para o volume. Os dados no volume são criptografados.

2. Verifique o status da operação de conversão:

   `volume encryption conversion show`

   Para a sintaxe de comando inteira, consulte a página man para o comando.

   O comando a seguir exibe o status da operação de conversão:

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   --------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Quando a operação de conversão estiver concluída, verifique se o volume está ativado para criptografia:

   `volume show -is-encrypted true`

   Para a sintaxe de comando inteira, consulte a página man para o comando.

   O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Resultado

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP automaticamente "envia" uma chave de criptografia para o servidor quando você criptografa um volume.

Ative a criptografia em um volume existente com o comando volume Move start

Você pode usar o `volume move start` comando para habilitar a criptografia movendo um volume existente. Você deve usar `volume move start` no ONTAP 9.2 e anterior. Você pode usar o mesmo agregado ou um agregado diferente.

Sobre esta tarefa

- A partir do ONTAP 9.8, pode utilizar `volume move start` para ativar a encriptação num volume SnapLock ou FlexGroup.
- A partir do ONTAP 9.4, se você ativar o "cc-mode" quando você configurar o Gerenciador de chaves integrado, os volumes criados com o `volume move start` comando serão automaticamente criptografados. Não é necessário especificar `-encrypt-destination true`.
- A partir do ONTAP 9.6, você pode usar a criptografia em nível de agregado para atribuir chaves ao agregado contendo para os volumes a serem movidos. Um volume criptografado com uma chave exclusiva é chamado de *volume NVE* (ou seja, usa criptografia de volume NetApp). Um volume criptografado com uma chave de nível agregado é chamado de *volume NAE* (para criptografia agregada NetApp). Os volumes de texto sem formatação não são suportados em agregados NAE.
- A partir do ONTAP 9.14,1, é possível criptografar um volume raiz do SVM com NVE. Para obter mais informações, Configurar o NetApp volume Encryption em um volume raiz da SVMconsulte .

Antes de começar

Você deve ser um administrador de cluster para executar essa tarefa ou um administrador SVM a quem o

administrador de cluster delegou autoridade.

"Delegando autoridade para executar o comando de movimentação de volume"

Passos

1. Mova um volume existente e especifique se a criptografia está ativada no volume:

Para converter…	Use este comando…
Um volume de texto sem formatação para um volume NVE	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
Um volume NVE ou de texto sem formatação para um volume NAE (assumindo que a criptografia no nível de agregado esteja ativada no destino)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
Um volume NAE para um volume NVE	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
Um volume NAE para um volume de texto sem formatação	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
Um volume NVE para um volume de texto sem formatação	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

Para a sintaxe de comando inteira, consulte a página man para o comando.

O comando a seguir converte um volume de texto sem formatação nomeado `vol1` em um volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Supondo que a criptografia em nível de agregado esteja ativada no destino, o comando a seguir converte um volume NVE ou de texto sem formatação nomeado `vol1` em um volume NAE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

O comando a seguir converte um volume NAE nomeado `vol2` em um volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

O comando a seguir converte um volume NAE nomeado `vol2` para um volume de texto sem formatação:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

O comando a seguir converte um volume NVE nomeado `vol2` em um volume de texto sem formatação:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Exibir o tipo de criptografia de volumes de cluster:

   `volume show -fields encryption-type none|volume|aggregate`

   O `encryption-type` campo está disponível no ONTAP 9.6 e posterior.

   Para a sintaxe de comando inteira, consulte a página man para o comando.

   O comando a seguir exibe o tipo de criptografia de volumes no `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Verifique se os volumes estão ativados para criptografia:

   `volume show -is-encrypted true`

   Para a sintaxe de comando inteira, consulte a página man para o comando.

   O comando a seguir exibe os volumes criptografados em `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Resultado

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP enviará automaticamente uma chave de criptografia ao servidor quando você criptografar um volume.

Configurar o NetApp volume Encryption em um volume raiz da SVM

A partir do ONTAP 9.14,1, é possível ativar o NetApp volume Encryption (NVE) em um volume raiz de VM de storage (SVM). Com o NVE, o volume raiz é criptografado com uma chave exclusiva, o que possibilita maior segurança no SVM.

Sobre esta tarefa

O NVE em um volume raiz do SVM só pode ser ativado após a criação do SVM.

Antes de começar

- O volume raiz do SVM não deve estar em um agregado criptografado com o NetApp Aggregate Encryption (NAE).
- Você deve ter habilitado a criptografia com o Gerenciador de chaves integrado ou um gerenciador de chaves externo.
- Você deve estar executando o ONTAP 9.14,1 ou posterior.
- Para migrar um SVM que contenha um volume raiz criptografado com NVE, você precisa converter o volume raiz do SVM em um volume de texto sem formatação após a conclusão da migração e, em seguida, criptografar novamente o volume raiz do SVM.
  - Se o agregado de destino da migração SVM usar NAE, o volume raiz herdará NAE por padrão.
- Se o SVM estiver em uma relação de recuperação de desastres do SVM:
  - As configurações de criptografia em um SVM espelhado não são copiadas para o destino. Se você ativar o NVE na origem ou no destino, habilite o NVE separadamente no volume raiz do SVM espelhado.
  - Se todos os agregados no cluster de destino usarem NAE, o volume raiz da SVM usará NAE.

Passos

Você pode ativar o NVE em um volume raiz da SVM com a CLI ou o Gerenciador de sistema do ONTAP.

CLI

Você pode ativar o NVE no volume raiz da SVM no local ou movendo o volume entre agregados.

Criptografe o volume raiz no lugar

1. Converta o volume raiz para um volume criptografado:

   `volume encryption conversion start -vserver` *`svm_name`* `-volume` *`volume`*

2. Confirme se a criptografia foi bem-sucedida. O `volume show -encryption-type volume` exibe uma lista de todos os volumes usando NVE.

Criptografe o volume raiz do SVM movendo-o.

1. Iniciar uma movimentação de volume:

   `volume move start -vserver` *`svm_name`* `-volume` *`volume`* `-destination-aggregate` *`aggregate`* `-encrypt-with-aggr-key false -encrypt-destination true`

   Para obter mais informações sobre `volume move`o , Mover um volumeconsulte .

2. Confirme se a `volume move` operação foi bem-sucedida com o `volume move show` comando. O `volume show -encryption-type volume` exibe uma lista de todos os volumes usando NVE.

System Manager

1. Navegue até **armazenamento** > **volumes**.
2. Ao lado do nome do volume raiz SVM que você deseja criptografar, selecione image:icon_kabob.gif<strong class=""Ícone de opções do menu"">Editar.
3. No título **armazenamento e Otimização**, selecione **Ativar criptografia**.
4. Selecione **Guardar**.

Habilite a criptografia de volume raiz do nó

A partir do ONTAP 9.8, você pode usar a criptografia de volume do NetApp para proteger o volume raiz do nó.

Sobre esta tarefa

Este procedimento aplica-se ao volume raiz do nó. Isso não se aplica aos volumes raiz do SVM. Os volumes de raiz da SVM podem ser protegidos com a criptografia no nível de agregado e, A partir do ONTAP 9.14,1, NVE.

Assim que a criptografia de volume raiz começar, ela deve ser concluída. Não é possível interromper a operação. Quando a criptografia estiver concluída, você não poderá atribuir uma nova chave ao volume raiz e não poderá executar uma operação de limpeza segura.

Antes de começar

- Seu sistema precisa estar usando uma configuração de HA.
- O volume raiz do nó já deve ser criado.
- Seu sistema precisa ter um gerenciador de chaves integrado ou um servidor externo de gerenciamento de chaves usando o Key Management Interoperability Protocol (KMIP).

Passos

1. Encriptar o volume raiz:

   `volume encryption conversion start -vserver SVM_name -volume root_vol_name`

2. Verifique o status da operação de conversão:

   `volume encryption conversion show`

3. Quando a operação de conversão estiver concluída, verifique se o volume está criptografado:

   `volume show -fields`

   A seguir mostra exemplos de saída para um volume criptografado.

```
::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
vserver    volume is-encrypted
---------- ------ ------------
xyz        vol0   true
```

Configurar a criptografia baseada em hardware do NetApp

Configure a visão geral da criptografia baseada em hardware do NetApp

A criptografia baseada em hardware da NetApp oferece suporte à criptografia de disco completo (FDE) dos dados conforme eles são gravados. Os dados não podem ser lidos sem uma chave de criptografia armazenada no firmware. A chave de criptografia, por sua vez, é acessível apenas para um nó autenticado.

Compreensão da criptografia baseada em hardware do NetApp

Um nó se autentica em uma unidade de autocriptografia usando uma chave de autenticação recuperada de um servidor de gerenciamento de chaves externo ou Gerenciador de chaves integrado:

- O servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que serve chaves para nós que usam o Key Management Interoperability Protocol (KMIP). É uma prática recomendada configurar servidores de gerenciamento de chaves externos em um sistema de armazenamento diferente dos seus dados.
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados.

Você pode usar a criptografia de volume do NetApp com criptografia baseada em hardware para "criptografar dados" em unidades com autocriptografia.

Quando as unidades de autocriptografia estão ativadas, o despejo de memória também é criptografado.

Se um par de HA estiver usando a criptografia de unidades SAS ou NVMe (SED, NSE, FIPS), siga as instruções no Retornar uma unidade FIPS ou SED para o modo desprotegido tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Tipos de unidade com autocriptografia compatíveis

Dois tipos de unidades com autocriptografia são compatíveis:

- As unidades SAS ou NVMe com certificação FIPS são compatíveis com todos os sistemas FAS e AFF. Essas unidades, chamadas unidades *FIPS,* estão em conformidade com os requisitos da publicação padrão Federal de processamento de informações 140-2, nível 2. Os recursos certificados habilitam proteções além da criptografia, como impedir ataques de negação de serviço na unidade. As unidades FIPS não podem ser combinadas com outros tipos de unidades no mesmo nó ou par de HA.
- A partir do ONTAP 9.6, as unidades NVMe com autocriptografia que não foram submetidas ao teste FIPS são compatíveis com sistemas AFF A800, A320 e posteriores. Essas unidades, chamadas *SEDs*, oferecem os mesmos recursos de criptografia que as unidades FIPS, mas podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.
- Todas as unidades validadas FIPS usam um módulo criptográfico de firmware que passou pela validação FIPS. O módulo criptográfico da unidade FIPS não usa nenhuma chave gerada fora da unidade (a senha de autenticação que é inserida na unidade é usada pelo módulo criptográfico de firmware da unidade para obter uma chave de criptografia de chave).

Unidades com autocriptografia são unidades que não são unidades FIPS ou SEDs.

Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Quando usar o gerenciamento de chaves externas

Embora seja mais barato e normalmente mais conveniente usar o gerenciador de chaves integrado, você deve usar o gerenciamento de chaves externas se alguma das seguintes opções for verdadeira:

- A política da sua organização requer uma solução de gerenciamento de chaves que use um módulo criptográfico FIPS 140-2 nível 2 (ou superior).
- Você precisa de uma solução de vários clusters, com gerenciamento centralizado de chaves de criptografia.
- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

Detalhes do suporte

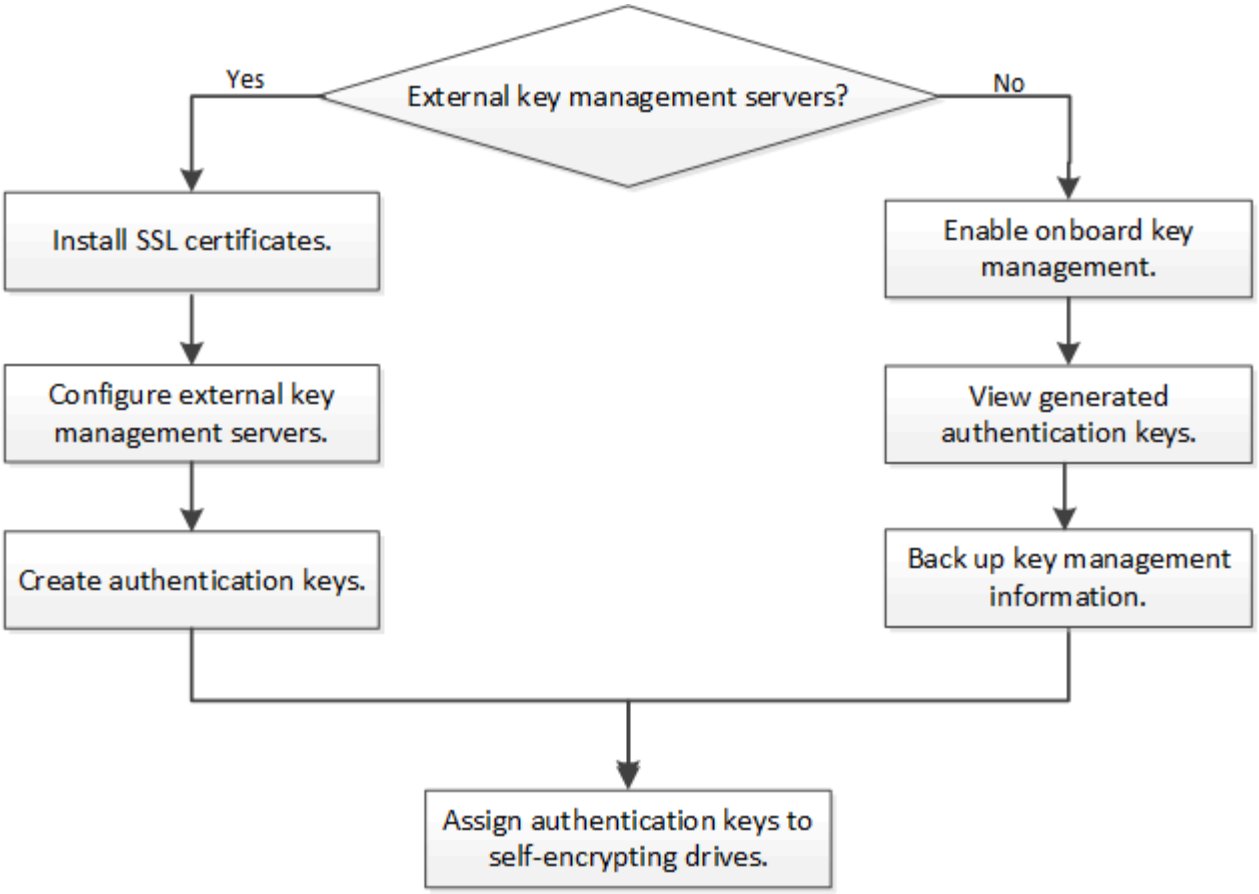
A tabela a seguir mostra detalhes importantes do suporte à criptografia de hardware. Consulte a Matriz de interoperabilidade para obter as informações mais recentes sobre servidores KMIP, sistemas de storage e compartimentos de disco compatíveis.

Recurso ou recurso	Detalhes do suporte

Conjuntos de discos não homogéneos	• As unidades FIPS não podem ser combinadas com outros tipos de unidades no mesmo nó ou par de HA. Pares de HA em conformidade podem coexistir com pares de HA não conformes no mesmo cluster. • As SEDs podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.
Tipo de unidade	• As unidades FIPS podem ser unidades SAS ou NVMe. • As SEDs devem ser unidades NVMe.
Interfaces de rede de 10 GB	A partir do ONTAP 9.3, as configurações de gerenciamento de chaves KMIP suportam interfaces de rede de 10 GB para comunicações com servidores de gerenciamento de chaves externas.
Portas para comunicação com o servidor de gerenciamento de chaves	A partir do ONTAP 9.3, você pode usar qualquer porta de controlador de armazenamento para comunicação com o servidor de gerenciamento de chaves. Caso contrário, você deve usar a porta e0M para comunicação com servidores de gerenciamento de chaves. Dependendo do modelo do controlador de storage, algumas interfaces de rede podem não estar disponíveis durante o processo de inicialização para comunicação com servidores de gerenciamento de chaves.
MetroCluster (MCC)	• As unidades NVMe são compatíveis com MCC. • As unidades SAS não suportam MCC.

Fluxo de trabalho de criptografia baseado em hardware

Você deve configurar os serviços de gerenciamento de chaves antes que o cluster possa se autenticar na unidade de autocriptografia. Você pode usar um servidor de gerenciamento de chaves externo ou um gerenciador de chaves integrado.



Informações relacionadas

- "NetApp Hardware Universe"
- "Criptografia de volumes do NetApp e criptografia agregada do NetApp"

Configurar o gerenciamento de chaves externas

Configurar uma visão geral do gerenciamento de chaves externas

Você pode usar um ou mais servidores de gerenciamento de chaves externos para proteger as chaves que o cluster usa para acessar dados criptografados. Um servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que serve chaves para nós que usam o Key Management Interoperability Protocol (KMIP).

Para o ONTAP 9.1 e versões anteriores, as LIFs de gerenciamento de nós devem ser atribuídas a portas configuradas com a função de gerenciamento de nó antes de usar o gerenciador de chaves externo.

O NetApp volume Encryption (NVE) pode ser implementado com o Gerenciador de chaves integrado no ONTAP 9.1 e posterior. No ONTAP 9.3 e posterior, o NVE pode ser implementado com gerenciamento de chaves externas (KMIP) e Gerenciador de chaves integrado. A partir do ONTAP 9.11,1, você pode configurar vários gerenciadores de chaves externos em um cluster. Consulte Configurar servidores de chaves em cluster.

Colete informações de rede no ONTAP 9.2 e anteriores

Se você estiver usando o ONTAP 9.2 ou anterior, você deve preencher a Planilha de

configuração de rede antes de ativar o gerenciamento de chaves externas.

> A partir do ONTAP 9.3, o sistema deteta automaticamente todas as informações de rede necessárias.

Item	Notas	Valor
Nome da interface de rede de gerenciamento de chaves		
Endereço IP da interface de rede de gerenciamento de chaves	Endereço IP do LIF de gerenciamento de nós, no formato IPv4 ou IPv6	
Comprimento do prefixo da rede IPv6 da interface de rede de gerenciamento de chaves	Se você estiver usando IPv6, o comprimento do prefixo de rede IPv6	
Máscara de sub-rede da interface de rede de gerenciamento de chaves		
Endereço IP do gateway de interface de rede de gerenciamento de chaves		
Endereço IPv6 para a interface de rede do cluster	Necessário somente se você estiver usando IPv6 para a interface de rede de gerenciamento de chaves	
Número da porta para cada servidor KMIP	Opcional. O número da porta deve ser o mesmo para todos os servidores KMIP. Se você não fornecer um número de porta, o padrão será a porta 5696, que é a porta atribuída pela IANA (Internet Assigned Numbers Authority) para KMIP.	
Nome da etiqueta da chave	Opcional. O nome da tag chave é usado para identificar todas as chaves pertencentes a um nó. O nome da etiqueta de chave padrão é o nome do nó.	

Informações relacionadas

"Relatório técnico da NetApp 3954: Requisitos e procedimentos de pré-instalação de criptografia de armazenamento da NetApp para o Gerenciador de chaves vitalício"

"Relatório técnico da NetApp 4074: Requisitos e procedimentos de pré-instalação da criptografia de armazenamento NetApp para o KeySecure"

Instale certificados SSL no cluster

O cluster e o servidor KMIP usam certificados SSL KMIP para verificar a identidade uns dos outros e estabelecer uma conexão SSL. Antes de configurar a conexão SSL com o servidor KMIP, você deve instalar os certificados SSL do cliente KMIP para o cluster e o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.

Sobre esta tarefa

Em um par de HA, ambos os nós precisam usar os mesmos certificados KMIP SSL públicos e privados. Se você conectar vários pares de HA ao mesmo servidor KMIP, todos os nós dos pares de HA precisarão usar os mesmos certificados KMIP SSL públicos e privados.

Antes de começar

- O tempo deve ser sincronizado no servidor criando os certificados, o servidor KMIP e o cluster.
- Você deve ter obtido o certificado de cliente KMIP SSL público para o cluster.
- Você deve ter obtido a chave privada associada ao certificado de cliente SSL KMIP para o cluster.
- O certificado de cliente SSL KMIP não deve ser protegido por senha.
- Você deve ter obtido o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.
- Em um ambiente MetroCluster, é necessário instalar os mesmos certificados SSL KMIP em ambos os clusters.

> Você pode instalar os certificados de cliente e servidor no servidor KMIP antes ou depois de instalar os certificados no cluster.

Passos

1. Instale os certificados de cliente SSL KMIP para o cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Você será solicitado a inserir os certificados SSL KMIP público e privado.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Instale o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Habilite o gerenciamento de chaves externas no ONTAP 9.6 e posterior (baseado em hardware)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. É possível conectar até quatro servidores KMIP a um nó. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

A partir do ONTAP 9.11,1, você pode adicionar até 3 servidores de chaves secundárias por servidor de chaves primárias para criar um servidor de chaves em cluster. Para obter mais informações, Configurar servidores de

chaves externas em clusterconsulte .

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

Passos

1. Configurar a conetividade do gerenciador de chaves para o cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   - O `security key-manager external enable` comando substitui o `security key-manager setup` comando. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas. Para obter a sintaxe completa do comando, consulte as páginas man.
   - Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para o SVM de administrador, repita o `security key-manager external enable` comando no cluster de parceiros.

   O comando a seguir habilita o gerenciamento de chaves externas para `cluster1` com três servidores de chaves externas. O primeiro servidor de chaves é especificado usando seu nome de host e porta, o segundo é especificado usando um endereço IP e a porta padrão, e o terceiro é especificado usando um endereço IPv6 e porta:

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Verifique se todos os servidores KMIP configurados estão conetados:

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   O `security key-manager external show-status` comando substitui o `security key-manager show -status` comando. Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  -------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores (baseado em hardware)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. É possível conectar até quatro servidores KMIP a um nó. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

Sobre esta tarefa

O ONTAP configura a conectividade do servidor KMIP para todos os nós no cluster.

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

Passos

1. Configurar a conectividade do gerenciador de chaves para nós de cluster:

   ```
   security key-manager setup
   ```

   A configuração do gerenciador de chaves é iniciada.

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

2. Insira a resposta apropriada em cada prompt.

3. Adicionar um servidor KMIP:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

4. Adicione um servidor KMIP adicional para redundância:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

5. Verifique se todos os servidores KMIP configurados estão conetados:

   `security key-manager show -status`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. Opcionalmente, converta volumes de texto simples em volumes criptografados.

   `volume encryption conversion start`

   Um gerenciador de chaves externo deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, um gerenciador de chaves externo deve ser configurado em ambos os locais.

Configurar servidores de chaves externas em cluster no ONTAP

A partir do ONTAP 9.11,1, é possível configurar a conetividade com servidores de gerenciamento de chaves externos em cluster em um SVM. Com servidores de chaves em cluster, você pode designar servidores de chaves primárias e secundárias em um SVM. Ao Registrar chaves, o ONTAP tentará primeiro acessar um servidor de chaves primárias antes de tentar acessar sequencialmente servidores secundários até que a

operação seja concluída com êxito, evitando a duplicação de chaves.

Os servidores de chaves externas podem ser usados para chaves NSE, NVE, NAE e SED. Um SVM pode dar suporte a até quatro servidores KMIP primários externos. Cada servidor principal pode suportar até três servidores de chaves secundárias.

Antes de começar

- "O gerenciamento de chaves KMIP deve estar habilitado para SVM".
- Esse processo só suporta servidores-chave que usam KMIP. Para obter uma lista de servidores de chaves suportados, verifique o "Ferramenta de Matriz de interoperabilidade do NetApp".
- Todos os nós no cluster devem estar executando o ONTAP 9.11,1 ou posterior.
- A ordem dos argumentos da lista de servidores no `-secondary-key-servers` parâmetro reflete a ordem de acesso dos servidores de gerenciamento de chaves externas (KMIP).
- Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP."

Crie um servidor de chaves em cluster

O procedimento de configuração depende se você configurou ou não um servidor de chave primária.

Adicionar servidores de chaves primárias e secundárias a uma SVM

1. Confirme se nenhum gerenciamento de chaves foi habilitado para o cluster:
   `security key-manager external show -vserver` *`svm_name`* Se o SVM já tiver o máximo de quatro servidores de chaves primárias ativados, você deverá remover um dos servidores de chaves primárias existentes antes de adicionar um novo.
2. Ative o gerenciador de chaves principal:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modifique o servidor de chaves primárias para adicionar servidores de chaves secundárias. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas de até três servidores-chave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Adicione servidores de chave secundária a um servidor de chave primária existente

1. Modifique o servidor de chaves primárias para adicionar servidores de chaves secundárias. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas de até três servidores-chave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`* Para obter mais informações sobre servidores de chaves secundárias, [mod-secondary]consulte .

Modificar servidores de chaves em cluster

Você pode modificar clusters de servidores de chave externos alterando o status (primário ou secundário) de servidores de chave específicos, adicionando e removendo servidores de chave secundária ou alterando a ordem de acesso de servidores de chave secundária.

Converta servidores de chaves primárias e secundárias

Para converter um servidor de chave primária em um servidor de chave secundário, primeiro remova-o do SVM com o `security key-manager external remove-servers` comando.

Para converter um servidor de chave secundária em um servidor de chave primária, primeiro você deve remover o servidor de chave secundária de seu servidor de chave primária existente. [mod-secondary]Consulte . Se você converter um servidor de chaves secundário para um servidor primário ao remover uma chave existente, tentar adicionar um novo servidor antes de concluir a remoção e conversão pode resultar na duplicação de chaves.

Modificar servidores de chaves secundárias

Os servidores de chaves secundárias são gerenciados com o `-secondary-key-servers` parâmetro `security key-manager external modify-server` do comando. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas. A ordem especificada dos servidores de chaves secundárias na lista determina a sequência de acesso para os servidores de chaves secundárias. A ordem de acesso pode ser modificada executando o comando `security key-manager external modify-server` com os servidores de chaves secundárias inseridos em uma sequência diferente.

Para remover um servidor de chave secundário, os `-secondary-key-servers` argumentos devem incluir os servidores de chave que você deseja manter ao omitir o que deve ser removido. Para remover todos os servidores de chaves secundárias, use o argumento `-`, significando nenhum.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/[`security key-manager external` ONTAP

Crie chaves de autenticação no ONTAP 9.6 e posterior

Você pode usar o `security key-manager key create` comando para criar as chaves de autenticação para um nó e armazená-las nos servidores KMIP configurados.

Sobre esta tarefa

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com FIPS usada para acesso aos dados.

O ONTAP cria chaves de autenticação para todos os nós no cluster.

- Este comando não é suportado quando o Onboard Key Manager está ativado. No entanto, duas chaves de autenticação são criadas automaticamente quando o Onboard Key Manager está ativado. As teclas podem ser visualizadas com o seguinte comando:

  ```
  security key-manager key query -key-type NSE-AK
  ```

- Você receberá um aviso se os servidores de gerenciamento de chaves configurados já estiverem armazenando mais de 128 chaves de autenticação.
- Você pode usar o `security key-manager key delete` comando para excluir quaisquer chaves não utilizadas. O `security key-manager key delete` comando falha se a chave dada estiver atualmente em uso pelo ONTAP. (Você deve ter Privileges maior que "'admin'" para usar este comando.)

Em um ambiente MetroCluster, antes de excluir uma chave, certifique-se de que a chave não está em uso no cluster de parceiros. Você pode usar os seguintes comandos no cluster de parceiros para verificar se a chave não está em uso:

- `storage encryption disk show -data-key-id key-id`
- `storage encryption disk show -fips-key-id key-id`

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Crie as chaves de autenticação para nós de cluster:

   `security key-manager key create -key-tag passphrase_label -prompt-for-key true|false`

   A configuração `prompt-for-key=true` faz com que o sistema solicite ao administrador do cluster a senha a ser usada ao autenticar unidades criptografadas. Caso contrário, o sistema gera automaticamente uma frase-passe de 32 bytes. O `security key-manager key create` comando substitui o `security key-manager create-key` comando. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria as chaves de autenticação para `cluster1`o , gerando automaticamente uma senha de 32 bytes:

   ```
   cluster1::> security key-manager key create
   Key ID:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b0000000000000000
   ```

2. Verifique se as chaves de autenticação foram criadas:

   `security key-manager key query -node node`

   O `security key-manager key query` comando substitui o `security key-manager query key` comando. Para obter a sintaxe completa do comando, consulte a página man. O ID da chave exibido na saída é um identificador usado para se referir à chave de autenticação. Não é a chave de autenticação real ou a chave de criptografia de dados.

   O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Crie chaves de autenticação no ONTAP 9.5 e anteriores

Você pode usar o `security key-manager create-key` comando para criar as chaves de autenticação para um nó e armazená-las nos servidores KMIP configurados.

Sobre esta tarefa

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

O ONTAP cria chaves de autenticação para todos os nós no cluster.

- Este comando não é suportado quando o gerenciamento de chaves integradas está habilitado.
- Você receberá um aviso se os servidores de gerenciamento de chaves configurados já estiverem

armazenando mais de 128 chaves de autenticação.

Você pode usar o software do servidor de gerenciamento de chaves para excluir quaisquer chaves não utilizadas e, em seguida, executar o comando novamente.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Crie as chaves de autenticação para nós de cluster:

   `security key-manager create-key`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   > O ID da chave exibido na saída é um identificador usado para se referir à chave de autenticação. Não é a chave de autenticação real ou a chave de criptografia de dados.

   O exemplo a seguir cria as chaves de autenticação para `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Verifique se as chaves de autenticação foram criadas:

   `security key-manager query`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED (gerenciamento de chaves externas)

Você pode usar o `storage encryption disk modify` comando para atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED. Os nós de cluster usam essa chave para bloquear ou desbloquear dados criptografados na unidade.

Sobre esta tarefa

Uma unidade com autocriptografia é protegida contra acesso não autorizado somente se o ID da chave de autenticação estiver definido como um valor não padrão. O ID seguro do fabricante (MSID), que tem ID de chave 0x0, é o valor padrão para unidades SAS. Para unidades NVMe, o valor padrão é uma chave nula, representada como um ID de chave em branco. Quando você atribui o ID da chave a uma unidade de autocriptografia, o sistema altera o ID da chave de autenticação para um valor não padrão.

Este procedimento não causa interrupções.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

Para obter a sintaxe de comando completa, consulte a página man para o comando.

> Você pode usar o `security key-manager query -key-type NSE-AK` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Verifique se as chaves de autenticação foram atribuídas:

   `storage encryption disk show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```

Configurar o gerenciamento de chaves integradas

Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior

Você pode usar o Gerenciador de chaves integrado para autenticar nós de cluster em uma unidade FIPS ou SED. O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados. O Gerenciador de chaves integrado é compatível com FIPS-140-2 nível 1.

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager onboard enable` comando sempre que adicionar um nó ao cluster. Nas configurações do MetroCluster, você deve executar `security key-manager onboard enable` primeiro no cluster local e, em seguida, executar `security key-manager onboard sync` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. Exceto no MetroCluster, você pode usar a `cc-mode-enabled=yes` opção para exigir que os usuários digitem a senha após uma reinicialização.

Quando o Gerenciador de chaves integrado está habilitado no modo Common Criteria (`cc-mode-enabled=yes`), o comportamento do sistema é alterado das seguintes maneiras:

- O sistema monitoriza as tentativas consecutivas de frase-passe do cluster falhadas ao funcionar no modo Common Criteria (critérios comuns).

  Se a encriptação de armazenamento NetApp (NSE) estiver ativada e não conseguir introduzir a frase-passe correta do cluster no arranque, o sistema não pode autenticar-se nas suas unidades e reinicia automaticamente. Para corrigir isso, você deve inserir a senha correta do cluster no prompt de inicialização. Uma vez iniciado, o sistema permite até 5 tentativas consecutivas para inserir corretamente a senha do cluster em um período de 24 horas para qualquer comando que exija a senha do cluster como um parâmetro. Se o limite for atingido (por exemplo, você não conseguiu inserir corretamente a senha do cluster 5 vezes em uma linha), então você deve esperar o período de tempo limite de 24 horas para decorrer, ou você deve reiniciar o nó, a fim de redefinir o limite.

- As atualizações de imagem do sistema usam o certificado de assinatura de código NetApp RSA-3072 juntamente com os digests assinados por código SHA-384 para verificar a integridade da imagem em vez do certificado de assinatura de código NetApp RSA-2048 usual e os digests assinados por código SHA-256.

  O comando upgrade verifica se o conteúdo da imagem não foi alterado ou corrompido verificando várias assinaturas digitais. O processo de atualização da imagem prossegue para o próximo passo se a validação for bem-sucedida; caso contrário, a atualização da imagem falhará. Consulte a página de manual ""imagem de cluster"" para obter informações sobre atualizações do sistema.

O Gerenciador de chaves integrado armazena as chaves na memória volátil. O conteúdo da memória volátil é apagado quando o sistema é reinicializado ou interrompido. Em condições normais de funcionamento, o conteúdo da memória volátil será apagado dentro de 30sMB quando um sistema for interrompido.

Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo.

  "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes que o Gerenciador de chaves integrado seja configurado.

Passos

1. Inicie o comando de configuração do gerenciador de chaves:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

Defina `cc-mode-enabled=yes` para exigir que os usuários inseram a senha do gerenciador de chaves após uma reinicialização. A `- cc-mode-enabled` opção não é suportada nas configurações do MetroCluster. O `security key-manager onboard enable` comando substitui o `security key-manager setup` comando.

O exemplo a seguir inicia o comando de configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

3. No prompt de confirmação da senha, redigite a senha.
4. Verifique se as chaves de autenticação foram criadas:

```
security key-manager key query -node node
```

O `security key-manager key query` comando substitui o `security key-manager query key` comando. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster. Você também deve fazer backup das informações manualmente para uso em caso de desastre.

Habilite o gerenciamento de chaves integradas no ONTAP 9.5 e versões anteriores

Você pode usar o Gerenciador de chaves integrado para autenticar nós de cluster em uma unidade FIPS ou SED. O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados. O Gerenciador de chaves integrado é compatível com FIPS-140-2 nível 1.

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar

dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo.

  "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes que o Gerenciador de chaves integrado seja configurado.

Passos

1. Inicie a configuração do gerenciador de chaves:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe do gestor de chaves após uma reinicialização. Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente.

   O exemplo a seguir inicia a configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Digite `yes` no prompt para configurar o gerenciamento de chaves integradas.
3. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

4. No prompt de confirmação da senha, redigite a senha.
5. Verifique se as chaves estão configuradas para todos os nós:

   `security key-manager key show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Depois de terminar

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "Faça backup manual das informações de gerenciamento de chaves integradas"Consulte .

Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED (gerenciamento de chaves integradas)

Você pode usar o `storage encryption disk modify` comando para atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED. Os nós de cluster usam essa chave para acessar dados na unidade.

Sobre esta tarefa

Uma unidade com autocriptografia é protegida contra acesso não autorizado somente se o ID da chave de autenticação estiver definido como um valor não padrão. O ID seguro do fabricante (MSID), que tem ID de chave 0x0, é o valor padrão para unidades SAS. Para unidades NVMe, o valor padrão é uma chave nula, representada como um ID de chave em branco. Quando você atribui o ID da chave a uma unidade de autocriptografia, o sistema altera o ID da chave de autenticação para um valor não padrão.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   > Você pode usar o `security key-manager key query -key-type NSE-AK` comando para exibir IDs de chave.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Verifique se as chaves de autenticação foram atribuídas:

   `storage encryption disk show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Atribuir uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS

Você pode usar o `storage encryption disk modify` comando com a `-fips-key-id` opção para atribuir uma chave de autenticação FIPS 140-2 a uma unidade FIPS. Os nós de cluster usam essa chave para operações de unidade que não sejam o acesso a dados, como impedir ataques de negação de serviço na unidade.

Sobre esta tarefa

Sua configuração de segurança pode exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

Este procedimento não causa interrupções.

Antes de começar

O firmware da unidade deve ser compatível com a conformidade FIPS 140-2-2. O "Ferramenta de Matriz de interoperabilidade do NetApp" contém informações sobre as versões de firmware da unidade suportadas.

Passos

1. Primeiro, você deve garantir que atribuiu uma chave de autenticação de dados. Isso pode ser feito com o uso de um gerenciador de chaves externo ou um gerenciador de chaves integrado. Verifique se a chave está atribuída com o comando `storage encryption disk show`.
2. Atribuir uma chave de autenticação FIPS 140-2 a SEDs:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   Você pode usar o `security key-manager query` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. Verifique se a chave de autenticação foi atribuída:

   `storage encryption disk show -fips`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Habilite o modo compatível com FIPS em todo o cluster para conexões de servidor KMIP

Você pode usar o `security config modify` comando com a `-is-fips-enabled` opção de ativar o modo compatível com FIPS em todo o cluster para dados em trânsito. Isso força o cluster a usar o OpenSSL no modo FIPS ao se conetar a servidores KMIP.

Sobre esta tarefa

Quando você ativa o modo compatível com FIPS em todo o cluster, o cluster usará automaticamente somente pacotes de codificação validados por FIPS e TLS1,2. O modo compatível com FIPS em todo o cluster está desativado por padrão.

Você deve reinicializar os nós de cluster manualmente após modificar a configuração de segurança em todo o cluster.

Antes de começar

- O controlador de storage deve ser configurado no modo compatível com FIPS.
- Todos os servidores KMIP precisam oferecer suporte a TLSv1,2. O sistema requer o TLSv1,2 para concluir a conexão com o servidor KMIP quando o modo compatível com FIPS em todo o cluster estiver ativado.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Verifique se o TLSv1,2 é suportado:

   `security config show -supported-protocols`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Ativar o modo compatível com FIPS em todo o cluster:

   `security config modify -is-fips-enabled true -interface SSL`

   Para obter a sintaxe completa do comando, consulte a página man.

4. Reinicializar os nós de cluster manualmente.
5. Verifique se o modo compatível com FIPS em todo o cluster está ativado:

   `security config show`

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

Gerenciar a criptografia NetApp

Descriptografe dados de volume

Você pode usar o `volume move start` comando para mover e descriptografar dados de volume.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "Delegar autoridade para executar o comando de movimentação de volume"consulte .

Passos

1. Mova um volume criptografado existente e descriptografe os dados no volume:

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   O comando a seguir move um volume existente nomeado `vol1` para o agregado de destino `aggr3` e descriptografa os dados no volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   O sistema exclui a chave de criptografia do volume. Os dados no volume não são criptografados.

2. Verifique se o volume está desativado para criptografia:

   `volume show -encryption`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   O comando a seguir exibe se os volumes em `cluster1` são criptografados:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Mover um volume criptografado

Você pode usar o `volume move start` comando para mover um volume criptografado. O volume movido pode residir no mesmo agregado ou em um agregado diferente.

Sobre esta tarefa

A movimentação falhará se o nó de destino ou o volume de destino não suportar criptografia de volume.

A `-encrypt-destination` opção para `volume move start` o padrão é verdadeiro para volumes criptografados. O requisito para especificar que não deseja que o volume de destino seja criptografado garante que você não descriptografe inadvertidamente os dados no volume.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "delegar autoridade para executar o comando de movimentação de volume"consulte .

Passos

1. Mova um volume criptografado existente e deixe os dados no volume criptografados:

`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

Para obter a sintaxe de comando completa, consulte a página man para o comando.

O comando a seguir move um volume existente nomeado `vol1` para o agregado de destino `aggr3` e deixa os dados no volume criptografados:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3
```

2. Verifique se o volume está ativado para criptografia:

`volume show -is-encrypted true`

Para obter a sintaxe de comando completa, consulte a página man para o comando.

O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

Delegar autoridade para executar o comando de movimentação de volume

Você pode usar o `volume move` comando para criptografar um volume existente, mover um volume criptografado ou descriptografar um volume. Os administradores de cluster podem executar `volume move` o comando sozinho ou delegar a autoridade para executar o comando aos administradores do SVM.

Sobre esta tarefa

Por padrão, a função é atribuída aos administradores de SVM `vsadmin`, que não inclui a autoridade para mover volumes. É necessário atribuir a `vsadmin-volume` função aos administradores do SVM para permitir que eles executem o `volume move` comando.

Passo

1. Delegar autoridade para executar o `volume move` comando:

`security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume`

Para obter a sintaxe de comando completa, consulte a página man para o comando.

O comando a seguir concede ao administrador SVM autoridade para executar o `volume move` comando.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

Altere a chave de criptografia de um volume com o comando de início de rechavear de criptografia de volume

É uma prática recomendada de segurança alterar a chave de criptografia para um volume periodicamente. A partir do ONTAP 9.3, você pode usar o `volume encryption rekey start` comando para alterar a chave de criptografia.

Sobre esta tarefa

Depois de iniciar uma operação de rechavear, ela deve ser concluída. Não há retorno à chave antiga. Se você encontrar um problema de desempenho durante a operação, você pode executar o `volume encryption rekey pause` comando para pausar a operação e o `volume encryption rekey resume` comando para retomar a operação.

Até que a operação de rechavear termine, o volume terá duas teclas. Novas gravações e suas leituras correspondentes usarão a nova chave. Caso contrário, as leituras usarão a chave antiga.

> Você não pode usar `volume encryption rekey start` para rechavear um volume SnapLock.

Passos

1. Alterar uma chave de encriptação:

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   O comando a seguir altera a chave de criptografia `vol1` no SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Verifique o estado da operação de rechavear:

   `volume encryption rekey show`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   O seguinte comando apresenta o estado da operação de rechavear:

   ```
   cluster1::> volume encryption rekey show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. Quando a operação de rechavear estiver concluída, verifique se o volume está ativado para encriptação:

   `volume show -is-encrypted true`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Altere a chave de criptografia de um volume com o comando volume Move start

É uma prática recomendada de segurança alterar a chave de criptografia para um volume periodicamente. Você pode usar o `volume move start` comando para alterar a chave de criptografia. Você deve usar `volume move start` no ONTAP 9.2 e anterior. O volume movido pode residir no mesmo agregado ou em um agregado diferente.

Sobre esta tarefa

Você não pode usar `volume move start` para rechavear um volume SnapLock ou FlexGroup.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "delegar autoridade para executar o comando de movimentação de volume"consulte .

Passos

1. Mova um volume existente e altere a chave de criptografia:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   O comando a seguir move um volume existente nomeado **`vol1`** para o agregado de destino **`aggr2`** e altera a chave de criptografia:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

   Uma nova chave de criptografia é criada para o volume. Os dados no volume permanecem criptografados.

2. Verifique se o volume está ativado para criptografia:

   `volume show -is-encrypted true`

Para obter a sintaxe de comando completa, consulte a página man para o comando.

O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Rode as chaves de autenticação para a encriptação de armazenamento NetApp

Você pode girar as chaves de autenticação ao usar a criptografia de armazenamento NetApp (NSE).

Sobre esta tarefa

A rotação de chaves de autenticação em um ambiente NSE é suportada se você estiver usando o KMIP (External Key Manager).

> A rotação de chaves de autenticação em um ambiente NSE não é compatível com OKM (Onboard Key Manager).

Passos

1. Use o `security key-manager create-key` comando para gerar novas chaves de autenticação.

   É necessário gerar novas chaves de autenticação antes de poder alterar as chaves de autenticação.

2. Use o `storage encryption disk modify -disk * -data-key-id` comando para alterar as chaves de autenticação.

Eliminar um volume encriptado

Você pode usar o `volume delete` comando para excluir um volume criptografado.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "delegar autoridade para executar o comando de movimentação de volume"consulte .
- O volume deve estar offline.

Passo

1. Eliminar um volume encriptado:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   O comando a seguir exclui um volume criptografado chamado `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Digite `yes` quando for solicitado que você confirme a exclusão.

O sistema exclui a chave de criptografia do volume após 24 horas.

Use `volume delete` com a `-force true` opção para excluir um volume e destruir a chave de criptografia correspondente imediatamente. Este comando requer Privileges avançado. Para obter mais informações, consulte a página de manual.

Depois de terminar

Você pode usar o `volume recovery-queue` comando para recuperar um volume excluído durante o período de retenção após a emissão do `volume delete` comando:

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"Como usar o recurso recuperação de volume"

Limpe os dados com segurança em um volume criptografado

Limpe os dados com segurança em uma visão geral de volume criptografado

A partir do ONTAP 9.4, você usa a limpeza segura para limpeza de dados em volumes habilitados para NVE sem interrupções. A análise de dados em um volume criptografado garante que ele não possa ser recuperado da Mídia física, por exemplo, em casos de "spillage", onde os rastreamentos de dados podem ter sido deixados para trás quando os blocos foram substituídos, ou para excluir com segurança os dados de um locatário em vazio.

A limpeza segura funciona apenas para arquivos excluídos anteriormente em volumes habilitados para NVE. Não é possível limpar um volume não criptografado. Você precisa usar servidores KMIP para fornecer chaves, não o gerenciador de chaves integrado.

Considerações sobre a utilização de uma purga segura

- Os volumes criados em um agregado habilitado para NetApp Aggregate Encryption (NAE) não oferecem suporte à limpeza segura.
- A limpeza segura funciona apenas para arquivos excluídos anteriormente em volumes habilitados para NVE.
- Não é possível limpar um volume não criptografado.
- Você precisa usar servidores KMIP para fornecer chaves, não o gerenciador de chaves integrado.

A limpeza segura funciona de forma diferente, dependendo da sua versão do ONTAP.

ONTAP 9 F.8 e mais tarde

- A purga segura é suportada pelo MetroCluster e pelo FlexGroup.
- Se o volume a ser purgado for a origem de uma relação SnapMirror, não é necessário interromper a relação SnapMirror para executar uma limpeza segura.
- O método de recriptografia é diferente para volumes que usam a proteção de dados do SnapMirror em vez de volumes que não usam a proteção de dados do SnapMirror (DP) ou aqueles que usam a proteção de dados estendida do SnapMirror.
  - Por padrão, os volumes que usam o modo de proteção de dados SnapMirror (DP) recriptografam os dados usando o método de recriptografia de movimentação de volume.
  - Por padrão, os volumes que não usam a proteção de dados SnapMirror ou volumes que usam o modo SnapMirror Extended Data Protection (XDP) usam o método de recriptografia no local.
  - Esses padrões podem ser alterados usando o `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Por padrão, todas as cópias Snapshot nos volumes FlexVol são automaticamente excluídas durante a operação de limpeza segura. Por padrão, os snapshots em volumes e volumes do FlexGroup que usam a proteção de dados do SnapMirror não são excluídos automaticamente durante a operação de limpeza segura. Esses padrões podem ser alterados usando o `secure purge delete-all-snapshots [true|false]` comando.

ONTAP 9.7 e anteriores:

- A purga segura não suporta o seguinte:
  - FlexClone
  - SnapVault
  - FabricPool
- Se o volume que está sendo purgado for a origem de uma relação do SnapMirror, você deve quebrar a relação do SnapMirror antes de poder limpar o volume.

  Se houver cópias snapshot ocupadas no volume, você precisará liberar as cópias Snapshot para poder limpar o volume. Por exemplo, talvez seja necessário dividir um volume FlexClone de seu pai.
- Chamar com êxito o recurso de limpeza segura aciona uma movimentação de volume que recriptografa os dados restantes e não limpos com uma nova chave.

  O volume movido permanece no agregado atual. A chave antiga é destruída automaticamente, garantindo que os dados purgados não possam ser recuperados da Mídia de armazenamento.

Limpe os dados com segurança em um volume criptografado sem uma relação com o SnapMirror

A partir do ONTAP 9.4, você pode usar a limpeza segura para dados "crostas" sem interrupções em volumes habilitados para NVE.

Sobre esta tarefa

A limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.

Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
   - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
   - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.
2. No sistema de armazenamento, altere para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

3. Se os arquivos que você deseja limpar com segurança estiverem em snapshots, exclua os snapshots:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Limpe com segurança os arquivos excluídos:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   O comando a seguir limpa com segurança os arquivos excluídos `vol1` no SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Verifique o estado da operação de purga segura:

   ```
   volume encryption secure-purge show
   ```

Limpe com segurança os dados em um volume criptografado com uma relação assíncrona do SnapMirror

A partir do ONTAP 9.8, você pode usar uma limpeza segura para dados "cruzadores" sem interrupções em volumes habilitados para NVE com uma relação assíncrona do SnapMirror.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Sobre esta tarefa

A limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.

> Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Passos

1. No sistema de armazenamento, mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
   - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
   - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.
3. Prepare o volume de destino na relação assíncrona para ser purgado com segurança:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Repita esta etapa em cada volume em sua relação assíncrona do SnapMirror.

4. Se os arquivos que você deseja limpar com segurança estiverem em cópias Snapshot, exclua as cópias Snapshot:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Se os arquivos que você deseja limpar com segurança estiverem nas cópias Snapshot base, faça o seguinte:

   a. Crie uma cópia Snapshot no volume de destino na relação assíncrona do SnapMirror:

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Atualize o SnapMirror para mover a cópia Snapshot base para frente:

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Repita esta etapa para cada volume na relação assíncrona do SnapMirror.

   a. Repita as etapas (a) e (b) iguais ao número de cópias Snapshot base mais uma.

      Por exemplo, se você tiver duas cópias Snapshot básicas, repita as etapas (a) e (b) três vezes.

   b. Verifique se a cópia Snapshot base está presente

```
snapshot show -vserver SVM_name -volume volume_name
```

c. Eliminar a cópia Snapshot base
```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

6. Limpe com segurança os arquivos excluídos:

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Repita esta etapa em cada volume na relação assíncrona do SnapMirror.

O seguinte comando limpa com segurança os arquivos excluídos no "'vol1" na SVM "'VS1":

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Verifique o estado da operação de purga segura:

```
volume encryption secure-purge show
```

Limpeza de dados em um volume criptografado com uma relação síncrona SnapMirror

A partir do ONTAP 9.8, você pode usar uma limpeza segura para "limpar" dados em volumes habilitados para NVE sem interrupções, com uma relação síncrona SnapMirror.

Sobre esta tarefa

Uma limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.

> Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. No sistema de armazenamento, altere para nível de privilégio avançado:

```
set -privilege advanced
```

2. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
   - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
   - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.

3. Prepare o volume de destino na relação assíncrona para ser purgado com segurança:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   Repita esta etapa para o outro volume em sua relação síncrona do SnapMirror.

4. Se os arquivos que você deseja limpar com segurança estiverem em cópias Snapshot, exclua as cópias Snapshot:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. Se o arquivo de limpeza segura estiver na base ou nas cópias Snapshot comuns, atualize o SnapMirror para mover a cópia Snapshot comum para frente:

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   Há duas cópias Snapshot comuns, portanto, esse comando deve ser emitido duas vezes.

6. Se o arquivo de limpeza segura estiver na cópia Snapshot consistente com o aplicativo, exclua a cópia Snapshot em ambos os volumes na relação síncrona do SnapMirror:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   Execute esta etapa em ambos os volumes.

7. Limpe com segurança os arquivos excluídos:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   Repita esta etapa em cada volume na relação síncrona do SnapMirror.

   O comando a seguir limpa com segurança os arquivos excluídos no "'vol1" no SVM "'VS1".

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Verifique o estado da operação de purga segura:

   ```
   volume encryption secure-purge show
   ```

Altere a senha de gerenciamento de chave integrada

É uma prática recomendada de segurança alterar periodicamente a senha de gerenciamento de chaves integradas. Copie a nova senha de gerenciamento de chaves integrada para um local seguro fora do sistema de storage para uso futuro.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

- São necessários Privileges avançados para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Altere a senha de gerenciamento de chaves integradas:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager onboard update-passphrase`
ONTAP 9 F.5 e anteriores	`security key-manager update-passphrase`

   Para obter a sintaxe completa do comando, consulte as páginas man.

   O seguinte comando ONTAP 9.6 permite alterar a senha de gerenciamento de chaves integradas para `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Digite `y` no prompt para alterar a senha de gerenciamento de chave integrada.
4. Introduza a frase-passe atual no prompt da frase-passe atual.
5. No novo prompt de senha, insira uma senha entre 32 e 256 carateres ou, para "cc-mode", uma senha entre 64 e 256 carateres.

   Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

6. No prompt de confirmação da senha, redigite a senha.

Depois de terminar

Em um ambiente MetroCluster, você deve atualizar a senha no cluster de parceiros:

- No ONTAP 9.5 e versões anteriores, é necessário executar `security key-manager update-passphrase` com a mesma senha no cluster de parceiros.
- No ONTAP 9.6 e posterior, você será solicitado a executar `security key-manager onboard sync` com a mesma senha no cluster de parceiros.

Copie a senha de gerenciamento de chaves integrada para um local seguro fora do sistema de storage para

uso futuro.

Você deve fazer backup manual das informações de gerenciamento de chaves sempre que alterar a senha de gerenciamento de chaves integradas.

"Fazer backup manual de informações de gerenciamento de chaves integradas"

Faça backup manual das informações de gerenciamento de chaves integradas

Você deve copiar as informações de gerenciamento de chaves integradas para um local seguro fora do sistema de armazenamento sempre que configurar a senha do Gerenciador de chaves integrado.

O que você vai precisar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Sobre esta tarefa

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster. Você também deve fazer backup manual das informações de gerenciamento de chaves para uso em caso de desastre.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Apresentar as informações de cópia de segurança da gestão de chaves para o cluster:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager onboard show-backup`
ONTAP 9 F.5 e anteriores	`security key-manager backup show`

Para obter a sintaxe completa do comando, consulte as páginas man.

O seguinte comando 9,6 exibe as informações de backup de gerenciamento de chaves `cluster1` para :

E

```
cluster1::> security key-manager onboard show-backup

      -------------------------BEGIN BACKUP-------------------------
      TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
      QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
      dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
      3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
      IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
      QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
      BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
      AQAAAAMAAAAYAQAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
      AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
      KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
      AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
      LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
      1cNLLwAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAkA
      ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAAJ4/cQsAAAAA
      AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAACQAAAAAAAA
      gAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
      rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      -------------------------END BACKUP-------------------------
```

1. Copie as informações de backup para um local seguro fora do sistema de armazenamento para uso em caso de desastre.

Restaurar chaves de criptografia integradas de gerenciamento de chaves

O procedimento a seguir para restaurar as chaves de criptografia integradas de gerenciamento de chaves varia de acordo com a versão do ONTAP.

Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo. Para obter mais informações, consulte "transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"
- Você deve ser um administrador de cluster para executar esta tarefa.

Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

ONTAP 9 F.6 e mais tarde

Se você estiver executando o ONTAP 9.8 ou posterior e o volume raiz estiver criptografado, siga o procedimento para [ontap-9-8].

1. Verifique se a chave precisa ser restaurada
   `security key-manager key query -node node`
2. Restaurar a chave
   `security key-manager onboard sync`

   Para obter a sintaxe completa do comando, consulte as páginas man.

   O seguinte comando ONTAP 9.6 sincroniza as chaves na hierarquia de chaves integradas:

```
cluster1::> security key-manager onboard sync

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
```

3. No prompt de frase-passe, insira a senha de gerenciamento de chave integrada para o cluster.

ONTAP 9.8 ou posterior com volume de raiz criptografado

Se você estiver executando o ONTAP 9.8 e posterior e seu volume raiz estiver criptografado, defina uma senha de recuperação de gerenciamento de chaves integrado com o menu de inicialização. Este processo também é necessário se você fizer uma substituição de Mídia de inicialização.

1. Inicialize o nó no menu de inicialização e selecione a opção `(10) Set onboard key management recovery secrets`.
2. Enter `y` para utilizar esta opção.
3. No prompt, insira a senha de gerenciamento de chaves integradas para o cluster.
4. No prompt, insira os dados da chave de backup.

   O nó retorna ao menu de inicialização.

5. No menu de inicialização, selecione a opção `(1) Normal Boot`.

ONTAP 9 F.5 e anteriores

1. Verifique se a chave precisa ser restaurada
   `security key-manager key show`
2. Se você estiver executando o ONTAP 9.8 e posterior e o volume raiz estiver criptografado, execute estas etapas:

   Se você estiver executando o ONTAP 9.6 ou 9,7, ou se estiver executando o ONTAP 9.8 ou posterior e o

volume raiz não estiver criptografado, pule esta etapa.

3. Restaurar a chave
`security key-manager setup -node node`

   Para obter a sintaxe completa do comando, consulte as páginas man.

4. No prompt de frase-passe, insira a senha de gerenciamento de chave integrada para o cluster.

Restaurar chaves de criptografia de gerenciamento de chaves externas

Você pode restaurar manualmente as chaves de criptografia de gerenciamento de chaves externas e enviá-las para um nó diferente. Você pode querer fazer isso se estiver reiniciando um nó que estava inativo temporariamente quando criou as chaves para o cluster.

Sobre esta tarefa

No ONTAP 9.6 e posterior, você pode usar o `security key-manager key query -node node_name` comando para verificar se sua chave precisa ser restaurada.

No ONTAP 9.5 e anteriores, você pode usar o `security key-manager key show` comando para verificar se sua chave precisa ser restaurada.

> Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Se você estiver executando o ONTAP 9.8 ou posterior e o volume raiz estiver criptografado, faça o seguinte:

   Se você estiver executando o ONTAP 9.7 ou anterior, ou se estiver executando o ONTAP 9.8 ou posterior e o volume raiz não estiver criptografado, pule esta etapa.

   a. Defina os bototargs
   ```
   setenv kmip.init.ipaddr <ip-address>
   setenv kmip.init.netmask <netmask>
   setenv kmip.init.gateway <gateway>
   setenv kmip.init.interface e0M
   boot_ontap
   ```

   b. Inicialize o nó no menu de inicialização e selecione a opção `(11) Configure node for external key management.`

   c. Siga as instruções para inserir o certificado de gerenciamento.

      Depois que todas as informações do certificado de gerenciamento forem inseridas, o sistema retornará ao menu de inicialização.

   d. No menu de inicialização, selecione a opção `(1) Normal Boot.`

2. Restaure a chave:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9 F.5 e anteriores

> `node` o padrão é todos os nós. Para obter a sintaxe completa do comando, consulte as páginas man. Este comando não é suportado quando o gerenciamento de chaves integradas está habilitado.

O seguinte comando ONTAP 9.6 restaura chaves de autenticação de gerenciamento de chaves externas para todos os nós no `cluster1`:

```
clusterl::> security key-manager external restore
```

Substitua os certificados SSL

Todos os certificados SSL têm uma data de validade. Você deve atualizar seus certificados antes que eles expirem para evitar a perda de acesso às chaves de autenticação.

Antes de começar

- Você precisa ter obtido o certificado público de substituição e a chave privada do cluster (certificado de cliente KMIP).
- Você deve ter obtido o certificado público de substituição para o servidor KMIP (certificado KMIP Server-CA).
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Se você estiver substituindo os certificados SSL KMIP em um ambiente MetroCluster, instale o mesmo certificado SSL KMIP de substituição em ambos os clusters.

> Você pode instalar os certificados de cliente e servidor de substituição no servidor KMIP antes ou depois de instalar os certificados no cluster.

Passos

1. Instale o novo certificado KMIP Server-CA:

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. Instale o novo certificado de cliente KMIP:

   ```
   security certificate install -type client -vserver <>
   ```

3. Atualize a configuração do gerenciador de chaves para usar os certificados recém-instalados:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
-certs <>
```

Se você estiver executando o ONTAP 9.6 ou posterior em um ambiente MetroCluster e quiser modificar a configuração do gerenciador de chaves no SVM admin, execute o comando nos dois clusters na configuração.

Atualizar a configuração do gerenciador de chaves para usar os certificados recém-instalados retornará um erro se as chaves públicas/privadas do novo certificado de cliente forem diferentes das chaves instaladas anteriormente. Consulte o artigo da base de dados de Conhecimento "As novas chaves públicas ou privadas do certificado de cliente são diferentes do certificado de cliente existente"para obter instruções sobre como substituir este erro.

Substitua uma unidade FIPS ou SED

Você pode substituir uma unidade FIPS ou SED da mesma forma que substitui um disco comum. Certifique-se de atribuir novas chaves de autenticação de dados à unidade de substituição. Para uma unidade FIPS, você também pode querer atribuir uma nova chave de autenticação FIPS 140-2-2.

Se um par de HA estiver usando "Criptografia de unidades SAS ou NVMe (SED, NSE, FIPS)", siga as instruções no "Retornar uma unidade FIPS ou SED para o modo desprotegido"tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Antes de começar

- Você deve saber o ID da chave para a chave de autenticação usada pela unidade.
- Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Certifique-se de que o disco foi marcado como com falha:

   ```
   storage disk show -broken
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Remova o disco com falha e substitua-o por uma nova unidade FIPS ou SED, seguindo as instruções no guia de hardware do modelo de compartimento de disco.
3. Atribua a propriedade do disco recém-substituído:

   `storage disk assign -disk disk_name -owner node`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Confirme se o novo disco foi atribuído:

   `storage encryption disk show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Atribua as chaves de autenticação de dados à unidade FIPS ou SED.

   "Atribuição de uma chave de autenticação de dados a uma unidade FIPS ou SED (gerenciamento de chaves externas)"

6. Se necessário, atribua uma chave de autenticação FIPS 140-2-2 à unidade FIPS.

   "Atribuição de uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS"

Tornar os dados em uma unidade FIPS ou SED inacessíveis

Torne os dados em uma unidade FIPS ou visão geral do SED inacessíveis

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis, mas manter o espaço não utilizado da unidade disponível para novos dados, você pode higienizar o disco. Se você quiser tornar os dados permanentemente inacessíveis e você não precisa reutilizar a unidade, você pode destruí-la.

- Sanitização de disco

  Quando você limpa uma unidade de autocriptografia, o sistema altera a chave de criptografia de disco para um novo valor aleatório, redefine o estado de bloqueio de inicialização para falso e define o ID da chave para um valor padrão, seja a ID segura do fabricante 0x0 (unidades SAS) ou uma chave nula (unidades NVMe). Isso torna os dados no disco inacessíveis e impossível de recuperar. Você pode reutilizar discos higienizados como discos sobressalentes não zerados.

- Destruição de disco

  Quando você destrói uma unidade FIPS ou SED, o sistema define a chave de criptografia de disco para um valor aleatório desconhecido e bloqueia o disco irreversivelmente. Isso torna o disco permanentemente inutilizável e os dados nele permanentemente inacessíveis.

Você pode higienizar ou destruir unidades de autocriptografia individuais ou todas as unidades de autocriptografia de um nó.

Higienize uma unidade FIPS ou SED

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis e usar a unidade para novos dados, use o `storage encryption disk sanitize` comando para higienizar a unidade.

Sobre esta tarefa

Quando você limpa uma unidade de autocriptografia, o sistema altera a chave de criptografia de disco para um novo valor aleatório, redefine o estado de bloqueio de inicialização para falso e define o ID da chave para um valor padrão, seja a ID segura do fabricante 0x0 (unidades SAS) ou uma chave nula (unidades NVMe). Isso torna os dados no disco inacessíveis e impossível de recuperar. Você pode reutilizar discos higienizados como discos sobressalentes não zerados.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Migre qualquer dado que precise ser preservado para um agregado em outro disco.
2. Exclua o agregado na unidade FIPS ou SED para ser higienizado:

   `storage aggregate delete -aggregate` *`aggregate_name`*

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifique a ID do disco para a unidade FIPS ou SED a ser higienizada:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Se uma unidade FIPS estiver em execução no modo de conformidade com FIPS, defina o ID da chave de autenticação FIPS para o nó novamente para o MSID padrão 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

Você pode usar o `security key-manager query` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Higienize a unidade:

```
storage encryption disk sanitize -disk disk_id
```

Você pode usar este comando para higienizar discos hot spare ou quebrados somente. Para higienizar todos os discos independentemente do tipo, use a `-force-all-state` opção. Para obter a sintaxe completa do comando, consulte a página man.

> O ONTAP solicitará que você insira uma frase de confirmação antes de continuar. Insira a frase exatamente como mostrado na tela.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Desfalhe o disco higienizado:
`storage disk unfail -spare true -disk disk_id`
7. Verifique se o disco tem um proprietário:
`storage disk show -disk disk_id` Se o disco não tem um proprietário, atribua um.
`storage disk assign -owner node -disk disk_id`
8. Introduza o nodeshell para o nó que possui os discos que pretende higienizar:

```
system node run -node node_name
```

Executar o `disk sanitize release` comando.

9. Saia do nodeshell. Desfalhe o disco novamente:
`storage disk unfail -spare true -disk disk_id`
10. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado:
`storage disk show -disk disk_id`

Destrua uma unidade FIPS ou SED

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis e não precisar reutilizar a unidade, use o `storage encryption disk destroy` comando para destruir o disco.

Sobre esta tarefa

Quando você destrói uma unidade FIPS ou SED, o sistema define a chave de criptografia de disco para um valor aleatório desconhecido e bloqueia a unidade irreversivelmente. Isso torna o disco praticamente inutilizável e os dados nele permanentemente inacessíveis. No entanto, você pode redefinir o disco para suas configurações configuradas de fábrica usando a ID física segura (PSID) impressa na etiqueta do disco. Para obter mais informações, "Retornar uma unidade FIPS ou SED ao serviço quando as chaves de autenticação são perdidas"consulte .

> Você não deve destruir uma unidade FIPS ou SED, a menos que tenha o serviço Non-Returnable Disk Plus (NRD Plus). Destruir um disco anula sua garantia.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Migre qualquer dado que precise ser preservado para um agregado em outro disco diferente.
2. Exclua o agregado na unidade FIPS ou SED a ser destruído:

   `storage aggregate delete -aggregate aggregate_name`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifique a ID do disco para a unidade FIPS ou SED a ser destruída:

   `storage encryption disk show`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Destrua o disco:

   ```
   storage encryption disk destroy -disk disk_id
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   > É-lhe pedido que introduza uma frase de confirmação antes de continuar. Insira a frase exatamente como mostrado na tela.

   ```
   cluster1::> storage encryption disk destroy -disk 1.10.2

   Warning: This operation will cryptographically destroy 1 spare or broken
            self-encrypting disks on 1 node.
            You cannot reuse destroyed disks unless you revert
            them to their original state using the PSID value.
            To continue, enter
             destroy disk
            :destroy disk

   Info: Starting destroy on 1 disk.
         View the status of the operation by using the
         "storage encryption disk show-status" command.
   ```

Dados de emergência cortados em uma unidade FIPS ou SED

Em caso de emergência de segurança, você pode impedir instantaneamente o acesso a uma unidade FIPS ou SED, mesmo que a energia não esteja disponível para o sistema de armazenamento ou para o servidor KMIP.

Antes de começar

- Se você estiver usando um servidor KMIP que não tem energia disponível, o servidor KMIP deve ser configurado com um item de autenticação facilmente destruído (por exemplo, um smart card ou unidade USB).
- Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Execute a fragmentação de emergência de dados em uma unidade FIPS ou SED:

Se…	Então…

A energia está disponível para o sistema de armazenamento e você tem tempo para colocar o sistema de armazenamento offline graciosamente	a. Se o sistema de storage estiver configurado como um par de HA, desative o takeover. b. Tire todos os agregados off-line e exclua-os. c. Defina o nível de privilégio como avançado `set -privilege advanced` d. Se a unidade estiver no modo de conformidade FIPS, defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão `storage encryption disk modify -disk * -fips-key-id 0x0` e. Parar o sistema de storage. f. Arranque no modo de manutenção. g. Sanitize ou destrua os discos: ◦ Se você quiser tornar os dados nos discos inacessíveis e ainda conseguir reutilizar os discos, limpe os discos `disk encrypt sanitize -all` ◦ Se você quiser tornar os dados nos discos inacessíveis e você não precisa salvar os discos, destrua os discos `disk encrypt destroy disk_id1 disk_id2 …`	A energia está disponível para o sistema de armazenamento e você deve destruir os dados imediatamente

a. **Se você quiser tornar os dados nos discos inacessíveis e ainda conseguir reutilizar os discos, higienize os discos:**
b. Se o sistema de storage estiver configurado como um par de HA, desative o takeover.
c. Defina o nível de privilégio como avançado:
`set -privilege advanced`
d. Se a unidade estiver no modo de conformidade FIPS, defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Higienizar o disco:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Se você quiser tornar os dados nos discos inacessíveis e não precisar salvar os discos, destrua os discos:**
	b. Se o sistema de storage estiver configurado como um par de HA, desative o takeover.
	c. Defina o nível de privilégio como avançado:
	`set -privilege advanced`
	d. Destrua os discos:
	`storage encryption disk destroy -disk * -force-all-states true`
		O sistema de armazenamento entra em pânico, deixando o sistema em um estado permanentemente desativado com todos os dados apagados. Para utilizar novamente o sistema, tem de o reconfigurar.

A energia está disponível para o servidor KMIP, mas não para o sistema de storage	a. Faça login no servidor KMIP. b. Destrua todas as chaves associadas às unidades FIPS ou SEDs que contenham os dados aos quais você deseja impedir o acesso. Isso impede o acesso a chaves de criptografia de disco pelo sistema de armazenamento.	A energia não está disponível para o servidor KMIP nem para o sistema de storage

Para obter a sintaxe completa do comando, consulte as páginas man.

Retorne uma unidade FIPS ou SED ao serviço usando o ONTAP quando as chaves de autenticação forem perdidas

O sistema trata uma unidade FIPS ou SED como quebrado se você perder as chaves de autenticação permanentemente e não conseguir recuperá-las do servidor KMIP. Embora você não possa acessar ou recuperar os dados no disco, você pode tomar medidas para

tornar o espaço não utilizado do SED disponível novamente para os dados.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Sobre esta tarefa

Deve utilizar este processo apenas se tiver a certeza de que as chaves de autenticação para a unidade FIPS ou SED estão permanentemente perdidas e que não pode recuperá-las.

Se os discos forem particionados, eles devem primeiro ser desparticionados antes de iniciar esse processo.

> O comando para desparticionar um disco só está disponível no nível de diag e só deve ser executado sob supervisão de suporte NetApp. **É altamente recomendável que você entre em Contato com o suporte da NetApp antes de prosseguir.** Você também pode consultar o artigo da base de dados de Conhecimento "Como desparticionar uma unidade sobressalente no ONTAP".

Passos

1. Retornar uma unidade FIPS ou SED à manutenção:

Se os SEDS são…	Siga estes passos…

Não está no modo de conformidade FIPS nem no modo de conformidade FIPS, e a chave FIPS está disponível	a. Defina o nível de privilégio como avançado:
	`set -privilege advanced`
	b. Reponha a chave FIPS para a ID segura de fabricação padrão 0x0:
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Verifique se a operação foi bem-sucedida:
	`storage encryption disk show-status` Se a operação falhou, use o processo PSID neste tópico.
	d. Sanitize o disco quebrado:
	`storage encryption disk sanitize -disk disk_id` Verifique se a operação foi bem-sucedida com o comando `storage encryption disk show-status` antes de prosseguir para a próxima etapa.
	e. Desfalhe o disco higienizado:
	`storage disk unfail -spare true -disk disk_id`
	f. Verifique se o disco tem um proprietário:
	`storage disk show -disk disk_id` Se o disco não tem um proprietário, atribua um.
	`storage disk assign -owner node -disk disk_id`
	i. Introduza o nodeshell para o nó que possui os discos que pretende higienizar:
	`system node run -node node_name`
	Executar o `disk sanitize release` comando.
	g. Saia do nodeshell. Desfalhe o disco novamente:
	`storage disk unfail -spare true -disk disk_id`
	h. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado:
	`storage disk show -disk disk_id`

No modo de conformidade com o FIPS, a chave FIPS não está disponível e os SEDs têm um PSID impresso na etiqueta	a. Obtenha o PSID do disco a partir da etiqueta do disco. b. Defina o nível de privilégio como avançado: `set -privilege advanced` c. Redefina o disco para suas configurações configuradas de fábrica: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Verifique se a operação foi bem-sucedida com o comando `storage encryption disk show-status` antes de prosseguir para a próxima etapa. d. Se você estiver executando o ONTAP 9.8P5 ou anterior, vá para a próxima etapa. Se você estiver executando o ONTAP 9.8P6 ou posterior, desmarque o disco higienizado. `storage disk unfail -disk` *`disk_id`* e. Verifique se o disco tem um proprietário: `storage disk show -disk` *`disk_id`* Se o disco não tem um proprietário, atribua um. `storage disk assign -owner node -disk` *`disk_id`* i. Introduza o nodeshell para o nó que possui os discos que pretende higienizar: `system node run -node` *`node_name`* Executar o `disk sanitize release` comando. f. Saia do nodeshell.. Desfalhe o disco novamente: `storage disk unfail -spare true -disk` *`disk_id`* g. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado: `storage disk show -disk` *`disk_id`*

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Retorne uma unidade FIPS ou SED para o modo desprotegido

Uma unidade FIPS ou SED é protegida contra acesso não autorizado somente se o ID da chave de autenticação para o nó estiver definido para um valor diferente do padrão. Você pode retornar uma unidade FIPS ou SED para o modo desprotegido usando o `storage encryption disk modify` comando para definir o ID da chave como padrão.

Se um par de HA estiver usando a criptografia de unidades SAS ou NVMe (SED, NSE, FIPS), siga este processo para todas as unidades dentro do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Se uma unidade FIPS estiver em execução no modo de conformidade com FIPS, defina o ID da chave de autenticação FIPS para o nó novamente para o MSID padrão 0x0:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   Você pode usar o `security key-manager query` comando para exibir IDs de chave.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Confirme a operação com sucesso com o comando:

   `storage encryption disk show-status`

   Repita o comando show-status até que os números em "discos iniciados" e "discos concluídos" sejam os mesmos.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start               Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp           Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------  ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Defina o ID da chave de autenticação de dados para o nó de volta para o MSID padrão 0x0:

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   O valor de `-data-key-id` deve ser definido como 0x0 se você estiver retornando uma unidade SAS ou NVMe para o modo desprotegido.

   Você pode usar o `security key-manager query` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confirme a operação com sucesso com o comando:

```
storage encryption disk show-status
```

Repita o comando show-status até que os números sejam os mesmos. A operação é concluída quando os números em "discos iniciados" e "discos concluídos" são os mesmos.

Modo de manutenção

Começando com ONTAP 9.7, você pode rechavear uma unidade FIPS a partir do modo de manutenção. Você só deve usar o modo de manutenção se não puder usar as instruções da CLI do ONTAP na seção anterior.

Passos

1. Defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão 0x0:

   ```
   disk encrypt rekey_fips 0x0 disklist
   ```

2. Defina o ID da chave de autenticação de dados para o nó de volta para o MSID padrão 0x0:

   ```
   disk encrypt rekey 0x0 disklist
   ```

3. Confirme se a chave de autenticação FIPS foi rekeyed com êxito:

   ```
   disk encrypt show_fips
   ```

4. Confirmar chave de autenticação de dados foi rekeyed com sucesso com:

   ```
   disk encrypt show
   ```

   Sua saída provavelmente exibirá o ID de chave padrão MSID 0x0 ou o valor de 64 carateres mantido pelo servidor de chaves. O `Locked?` campo refere-se ao bloqueio de dados.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Remova uma conexão externa do gerenciador de chaves

Você pode desconetar um servidor KMIP de um nó quando não precisar mais do servidor. Por exemplo, você pode desconetar um servidor KMIP quando estiver migrando para a criptografia de volume.

Sobre esta tarefa

Ao desconetar um servidor KMIP de um nó em um par de HA, o sistema desconeta automaticamente o servidor de todos os nós de cluster.

> Se você pretende continuar usando o gerenciamento de chaves externas depois de desconetar um servidor KMIP, verifique se outro servidor KMIP está disponível para servir as chaves de autenticação.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Desconete um servidor KMIP do nó atual:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9 F.5 e anteriores

Em um ambiente do MetroCluster, você deve repetir esses comandos nos dois clusters para o SVM de administrador.

Para obter a sintaxe completa do comando, consulte as páginas man.

O seguinte comando ONTAP 9.6 desativa as conexões a dois servidores de gerenciamento de chaves externas para `cluster1`, o primeiro chamado `ks1`, ouvindo na porta padrão 5696, o segundo com o endereço IP 10,0.0,20, ouvindo na porta 24482:

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Modifique as propriedades do servidor de gerenciamento de chaves externas

A partir do ONTAP 9.6, você pode usar o `security key-manager external modify-server` comando para alterar o tempo limite de e/S e o nome de usuário de um servidor de gerenciamento de chaves externo.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- São necessários Privileges avançados para esta tarefa.
- Em um ambiente do MetroCluster, repita essas etapas nos dois clusters para o SVM de administrador.

Passos

1. No sistema de armazenamento, altere para nível de privilégio avançado:

```
set -privilege advanced
```

2. Modifique as propriedades do servidor do gerenciador de chaves externo para o cluster:

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> O valor de tempo limite é expresso em segundos. Se você modificar o nome de usuário, será solicitado que você insira uma nova senha. Se você executar o comando no prompt de login do cluster, *admin_SVM* o padrão será o administrador SVM do cluster atual. Você deve ser o administrador do cluster para modificar as propriedades do servidor do gerenciador de chaves externo.

O comando a seguir altera o valor de tempo limite para 45 segundos para que o `cluster1` servidor de gerenciamento de chaves externo esteja escutando na porta padrão 5696:

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. Modificar as propriedades do servidor do gerenciador de chaves externo para uma SVM (somente NVE):

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> O valor de tempo limite é expresso em segundos. Se você modificar o nome de usuário, será solicitado que você insira uma nova senha. Se você executar o comando no prompt de login SVM, *SVM* o padrão será SVM atual. Você deve ser o administrador do cluster ou SVM para modificar as propriedades do servidor do gerenciador de chaves externo.

O comando a seguir altera o nome de usuário e a senha do `svm1` servidor de gerenciamento de chaves externo ouvindo na porta padrão 5696:

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. Repita a última etapa para quaisquer SVMs adicionais.

Transição para o gerenciamento de chaves externas do gerenciamento de chaves integrado

Se você quiser alternar para o gerenciamento de chaves externas do gerenciamento de chaves integradas, exclua a configuração de gerenciamento de chaves integradas antes de habilitar o gerenciamento de chaves externas.

Antes de começar

- Para criptografia baseada em hardware, é necessário redefinir as chaves de dados de todas as unidades FIPS ou SEDs para o valor padrão.

"Retornar uma unidade FIPS ou SED para o modo desprotegido"

- Para criptografia baseada em software, você deve descriptografar todos os volumes.

  "Uncriptografando dados de volume"

- Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Exclua a configuração de gerenciamento de chaves integradas para um cluster:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager onboard disable -vserver SVM`
ONTAP 9 F.5 e anteriores	`security key-manager delete-key-database`

Para obter a sintaxe de comando completa, consulte "Referência do comando ONTAP" .

Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas

Se você quiser alternar para o gerenciamento de chaves integradas do gerenciamento de chaves externas, exclua a configuração de gerenciamento de chaves externas para ativar o gerenciamento de chaves integradas.

Antes de começar

- Para criptografia baseada em hardware, é necessário redefinir as chaves de dados de todas as unidades FIPS ou SEDs para o valor padrão.

  "Retornar uma unidade FIPS ou SED para o modo desprotegido"

- Você deve ter excluído todas as conexões externas do gerenciador de chaves.

  "Excluindo uma conexão externa do gerenciador de chaves"

- Você deve ser um administrador de cluster para executar esta tarefa.

Procedimento

As etapas para fazer a transição do gerenciamento de chaves dependem da versão do ONTAP que você está usando.

ONTAP 9 F.6 e mais tarde

1. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Use o comando:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   Em um ambiente MetroCluster, você deve repetir o comando nos dois clusters para o SVM de administrador.

ONTAP 9 F.5 e anteriores

Use o comando:
`security key-manager delete-kmip-config`

O que acontece quando os servidores de gerenciamento de chaves não são alcançáveis durante o processo de inicialização

O ONTAP toma certas precauções para evitar um comportamento indesejado caso um sistema de armazenamento configurado para NSE não alcance nenhum dos servidores de gerenciamento de chaves especificados durante o processo de inicialização.

Se o sistema de armazenamento estiver configurado para NSE, os SEDs são rekeyed e locked e os SEDs são ligados, o sistema de armazenamento deve recuperar as chaves de autenticação necessárias dos servidores de gerenciamento de chaves para se autenticar nos SEDs antes de poder acessar os dados.

O sistema de armazenamento tenta contactar os servidores de gestão de chaves especificados durante até três horas. Se o sistema de armazenamento não puder alcançar nenhum deles depois desse tempo, o processo de inicialização será interrompido e o sistema de armazenamento será interrompido.

Se o sistema de armazenamento entrar em Contato com qualquer servidor de gerenciamento de chaves especificado, ele tentará estabelecer uma conexão SSL por até 15 minutos. Se o sistema de armazenamento não puder estabelecer uma conexão SSL com qualquer servidor de gerenciamento de chaves especificado, o processo de inicialização será interrompido e o sistema de armazenamento será interrompido.

Enquanto o sistema de armazenamento tenta entrar em Contato e se conetar a servidores de gerenciamento de chaves, ele exibe informações detalhadas sobre as tentativas de Contato com falha na CLI. Você pode interromper as tentativas de Contato a qualquer momento pressionando Ctrl-C.

Como medida de segurança, os SEDs permitem apenas um número limitado de tentativas de acesso não autorizado, após o qual desativam o acesso aos dados existentes. Se o sistema de armazenamento não puder contactar qualquer servidor de gestão de chaves especificado para obter as chaves de autenticação adequadas, só poderá tentar autenticar com a chave predefinida, o que leva a uma tentativa de falha e a um pânico. Se o sistema de armazenamento estiver configurado para reiniciar automaticamente em caso de pânico, ele entra em um loop de inicialização que resulta em tentativas de autenticação com falha contínua nos SEDs.

Parar o sistema de armazenamento nesses cenários é por projeto para impedir que o sistema de armazenamento entre em um loop de inicialização e possível perda não intencional de dados como resultado dos SEDs bloqueados permanentemente devido a exceder o limite de segurança de um certo número de

tentativas consecutivas de autenticação falhadas. O limite e o tipo de proteção de bloqueio dependem das especificações de fabricação e do tipo de SED:

Tipo de SED	Número de tentativas consecutivas falhadas de autenticação, resultando em bloqueio	Tipo de proteção de bloqueio quando o limite de segurança é atingido
HDD	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
X440_PHM2800MCTO 800GB SSDs NSE com revisões de firmware NA00 ou NA01	5	Temporário. O bloqueio só está em vigor até que o disco seja ligado a um ciclo de energia.
X577_PHM2800MCTO 800GB SSDs NSE com revisões de firmware NA00 ou NA01	5	Temporário. O bloqueio só está em vigor até que o disco seja ligado a um ciclo de energia.
X440_PHM2800MCTO 800GB SSDs NSE com revisões de firmware mais altas	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
X577_PHM2800MCTO 800GB SSDs NSE com revisões de firmware mais altas	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
Todos os outros modelos de SSD	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.

Para todos os tipos de SED, uma autenticação bem-sucedida redefine a contagem de tentativas para zero.

Se você encontrar este cenário em que o sistema de armazenamento é interrompido devido a falha em alcançar qualquer servidor de gerenciamento de chaves especificado, primeiro você deve identificar e corrigir a causa da falha de comunicação antes de tentar continuar inicializando o sistema de armazenamento.

Desative a criptografia por padrão

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo. Se necessário, você pode desativar a criptografia por padrão para todo o cluster.

Antes de começar

Você deve ser um administrador de cluster para executar essa tarefa ou um administrador SVM a quem o administrador de cluster delegou autoridade.

Passo

1. Para desativar a criptografia por padrão para todo o cluster no ONTAP 9.7 ou posterior, execute o seguinte comando:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

Ative o modelo Zero Trust

NetApp e confiança zero

O Zero Trust tradicionalmente tem sido uma abordagem centrada na rede de arquitetura de micro núcleo e perímetro (MCAP) para proteger dados, serviços, aplicativos ou ativos com controles conhecidos como gateway de segmentação. A NetApp ONTAP está adotando uma abordagem centrada em dados para a confiança zero, na qual o sistema de gerenciamento de storage se torna o gateway de segmentação para proteger e monitorar o acesso aos dados de nossos clientes. Em particular, o mecanismo FPolicy Zero Trust e o ecossistema parceiro da FPolicy se tornam um centro de controle para obter uma compreensão detalhada dos padrões de acesso a dados normais e aberrantes e identificar ameaças internas.

A partir de julho de 2024, o conteúdo do relatório técnico *TR-4829: NetApp e confiança zero: Habilitando um modelo de confiança zero centrado em dados*, que foi publicado anteriormente como PDF, foi integrado com o restante da documentação do produto ONTAP.

Os dados são o ativo mais importante que sua organização tem. As ameaças internas são a causa de 18% das violações de dados, de acordo com o 2022 "Relatório de investigações de violação de dados da Verizon". As organizações podem aumentar a vigilância com a implantação de controles de confiança zero líderes do setor relacionados aos dados com o software de gerenciamento de dados NetApp ONTAP.

O que é Zero Trust?

O modelo Zero Trust foi desenvolvido pela primeira vez por John Kindervag na Forrester Research. A abordagem Zero Trust de dentro para fora identifica um micronúcleo e um perímetro (MCAP). O MCAP é uma definição interior de dados, serviços, aplicativos e ativos a serem protegidos com um conjunto abrangente de controles. O conceito de um perímetro externo seguro é obsoleto. As entidades que são confiáveis e têm permissão para se autenticar com êxito através do perímetro podem então tornar a organização vulnerável a ataques. Insiders, por definição, já estão dentro do perímetro seguro. Funcionários, contratados e parceiros são membros da equipe e precisam estar habilitados a operar com controles apropriados para desempenhar suas funções na infraestrutura da organização.

Zero Trust foi mencionado como uma tecnologia que oferece promessa ao DoD em setembro de 2019 "FY19-23 Estratégia de modernização Digital DoD". Ele define Zero Trust como "Uma estratégia de segurança cibernética que incorpora segurança em toda a arquitetura com o objetivo de impedir violações de dados. Esse modelo de segurança centrado em dados elimina a ideia de redes, dispositivos, personas ou processos confiáveis ou não confiáveis e muda para níveis de confiança baseados em múltiplos atributos que permitem políticas de autenticação e autorização sob o conceito de acesso menos privilegiado. A implementação de confiança zero requer repensar a forma como utilizamos a infraestrutura existente para implementar a segurança através do design de uma forma mais simples e eficiente, ao mesmo tempo que permite operações desimpedidas."

Em agosto de 2020, o NIST publicou "Especial Pub 800-207 arquitetura Zero Trust" (ZTA). O ZTA se concentra em proteger recursos, não segmentos de rede, porque a localização da rede não é mais vista como o principal componente da postura de segurança do recurso. Os recursos são dados e computação. As estratégias ZTA são para arquitetos de rede empresarial. O ZTA introduz uma nova terminologia dos conceitos originais da Forrester. Os mecanismos de proteção chamados de ponto de decisão de política (PDP) e ponto de aplicação de políticas (PEP) são análogos a um gateway de segmentação da Forrester. A ZTA apresenta quatro modelos de implantação:

- Implantação baseada em agente de dispositivo ou gateway
- Implantação baseada em enclave (um pouco análoga ao Forrester MCAP)
- Implantação baseada em portal de recursos
- Aplicação do dispositivo sandboxing

Para os fins desta documentação, usamos os conceitos e a terminologia da Forrester Research em vez do ZTA NIST.

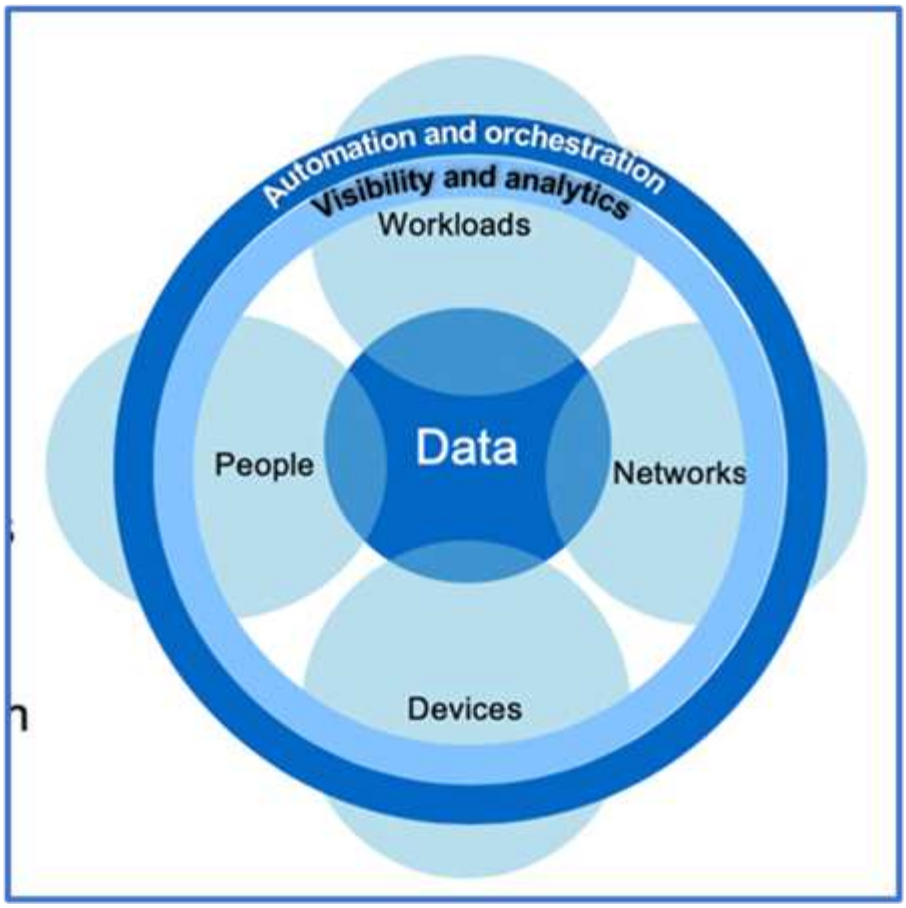
Recursos de segurança

Para obter informações sobre como reportar vulnerabilidades e incidentes, respostas de segurança do NetApp e confidencialidade do cliente, consulte o "Portal de segurança da NetApp".

Projete uma abordagem centrada em dados para zero confiança com o ONTAP

Uma rede Zero Trust é definida por uma abordagem centrada em dados, na qual os controles de segurança devem estar o mais próximos possível dos dados. As funcionalidades do ONTAP, somadas ao ecossistema parceiro do NetApp FPolicy, podem fornecer os controles necessários para o modelo de confiança zero centrado em dados.

O ONTAP é um software de gerenciamento de dados seguro da NetApp, e o mecanismo de confiança zero da FPolicy é um recurso ONTAP líder do setor que oferece uma interface de notificação granular com eventos baseados em arquivo. Os parceiros do NetApp FPolicy podem usar essa interface para fornecer mais informações sobre o acesso aos dados no ONTAP.



Crie um MCAP centrado em dados Zero Trust

Para arquitetar um MCAP Zero Trust centrado em dados, siga estas etapas:

1. Identificar a localização de todos os dados organizacionais.
2. Classificar os dados.
3. Elimine com segurança os dados que já não necessita.
4. Entenda quais funções devem ter acesso às classificações de dados.
5. Aplique o princípio de privilégio mínimo para aplicar controles de acesso.
6. Use a autenticação multifator para acesso administrativo e acesso aos dados.
7. Uso de criptografia para dados em repouso e dados em trânsito.
8. Monitore e Registre todo o acesso.
9. Alertar acessos ou comportamentos suspeitos.

Identificar a localização de todos os dados organizacionais

O recurso FPolicy do ONTAP, juntamente com o ecossistema de parceiros da Aliança NetApp dos parceiros FPolicy, permite identificar onde os dados da sua organização existem e quem tem acesso a eles. Isso é feito com análise comportamental do usuário, que identifica se os padrões de acesso aos dados são válidos. Mais detalhes sobre a análise comportamental do usuário são discutidos no Monitor e log todo o acesso. Se você não entender onde seus dados estão e quem tem acesso a eles, a análise comportamental do usuário pode fornecer uma linha de base para criar classificação e política a partir de observações empíricas.

Classificar os dados

Na terminologia do modelo Zero Trust, a classificação dos dados envolve a identificação de dados tóxicos. Dados tóxicos são dados confidenciais que não se destinam a ser expostos fora de uma organização. A divulgação de dados tóxicos pode violar a conformidade regulamentar e prejudicar a reputação de uma organização. Em termos de conformidade regulamentar, os dados tóxicos incluem dados do titular do cartão para a, dados pessoais para a "Padrão de segurança de dados do setor de cartões de pagamento (PCI-DSS)" UE "Regulamento Geral de proteção de dados (GDPR)" ou dados de cuidados de saúde para a "Lei de portabilidade e responsabilidade de seguros de saúde (HIPAA)". Você pode usar o NetApp "Classificação BlueXP " (anteriormente conhecido como Cloud Data Sense), um kit de ferramentas orientado por IA, para verificar, analisar e categorizar automaticamente seus dados.

Elimine com segurança os dados que já não necessita

Depois de classificar os dados da sua organização, você pode descobrir que alguns dos seus dados não são mais necessários ou relevantes para a função da sua organização. A retenção de dados desnecessários é uma responsabilidade, e esses dados devem ser excluídos. Para obter um mecanismo avançado para apagar dados criptograficamente, consulte a descrição da limpeza segura na criptografia dados em repouso.

Entenda quais funções devem ter acesso às classificações de dados e aplique o princípio de menor privilégio para impor controles de acesso

Mapear o acesso a dados confidenciais e aplicar o princípio do menor privilégio significa dar às pessoas em sua organização acesso apenas aos dados necessários para executar seus trabalhos. Esse processo envolve controle de acesso baseado em função ("RBAC"), que se aplica ao acesso a dados e acesso administrativo.

Com o ONTAP, uma máquina virtual de storage (SVM) pode ser usada para segmentar o acesso a dados organizacionais por locatários em um cluster do ONTAP. O RBAC pode ser aplicado ao acesso aos dados, bem como ao acesso administrativo ao SVM. O RBAC também pode ser aplicado no nível administrativo do cluster.

Além do RBAC, você pode usar o ONTAP "verificação multi-admin"(MAV) para exigir que um ou mais administradores aprovem comandos como `volume delete` ou `volume snapshot delete`. Uma vez que o MAV está ativado, modificar ou desativar o MAV requer a aprovação do administrador do MAV.

Outra maneira de proteger as cópias Snapshot é com o ONTAP "Bloqueio de cópias snapshot". O bloqueio de cópias snapshot é uma funcionalidade do SnapLock em que as cópias Snapshot são tornadas indeléveis manual ou automaticamente, com um período de retenção na política de cópia Snapshot de volume. O bloqueio de cópias snapshot também é conhecido como bloqueio de cópias Snapshot à prova de violação. O objetivo do bloqueio de cópias Snapshot é impedir que administradores desonestos ou não confiáveis excluam cópias Snapshot nos sistemas ONTAP primário e secundário. A recuperação rápida de cópias Snapshot bloqueadas em sistemas primários pode ser obtida para restaurar volumes corrompidos por ransomware.

Use a autenticação multifator para acesso administrativo e acesso aos dados

Além do RBAC administrativo de cluster, "Autenticação de vários fatores (MFA)" pode ser implantado para acesso à linha de comando ONTAP web administrative Access e Secure Shell (SSH). O MFA para acesso administrativo é um requisito para organizações do setor público dos EUA ou aquelas que precisam seguir o PCI-DSS. O MFA torna impossível para um invasor comprometer uma conta usando apenas um nome de usuário e senha. O MFA requer dois ou mais fatores independentes para autenticar. Um exemplo de autenticação de dois fatores é algo que um usuário possui, como uma chave privada, e algo que um usuário conhece, como uma senha. O acesso administrativo à Web ao ONTAP System Manager ou ao ActiveIQ Unified Manager é habilitado pela Security Assertion Markup Language (SAML) 2,0. O acesso à linha de comando SSH usa autenticação de dois fatores encadeada com uma chave pública e uma senha.

Você pode controlar o acesso de usuário e máquina por meio de APIs com os recursos de gerenciamento de identidade e acesso no ONTAP:

- Utilizador:
  - **Autenticação e autorização.** Por meio de funcionalidades de protocolo nas para SMB e NFS.
  - **Auditoria.** Syslog de acessos e eventos. Registo de auditoria detalhado do protocolo CIFS para testar políticas de autenticação e autorização. Auditoria granular fina de FPolicy de acesso detalhado nas no nível do arquivo.
- Dispositivo:
  - **Autenticação.** Autenticação baseada em certificado para acesso à API.
  - **Autorização.** Controle de acesso padrão ou personalizado baseado em função (RBAC).
  - **Auditoria.** Syslog de todas as ações tomadas.

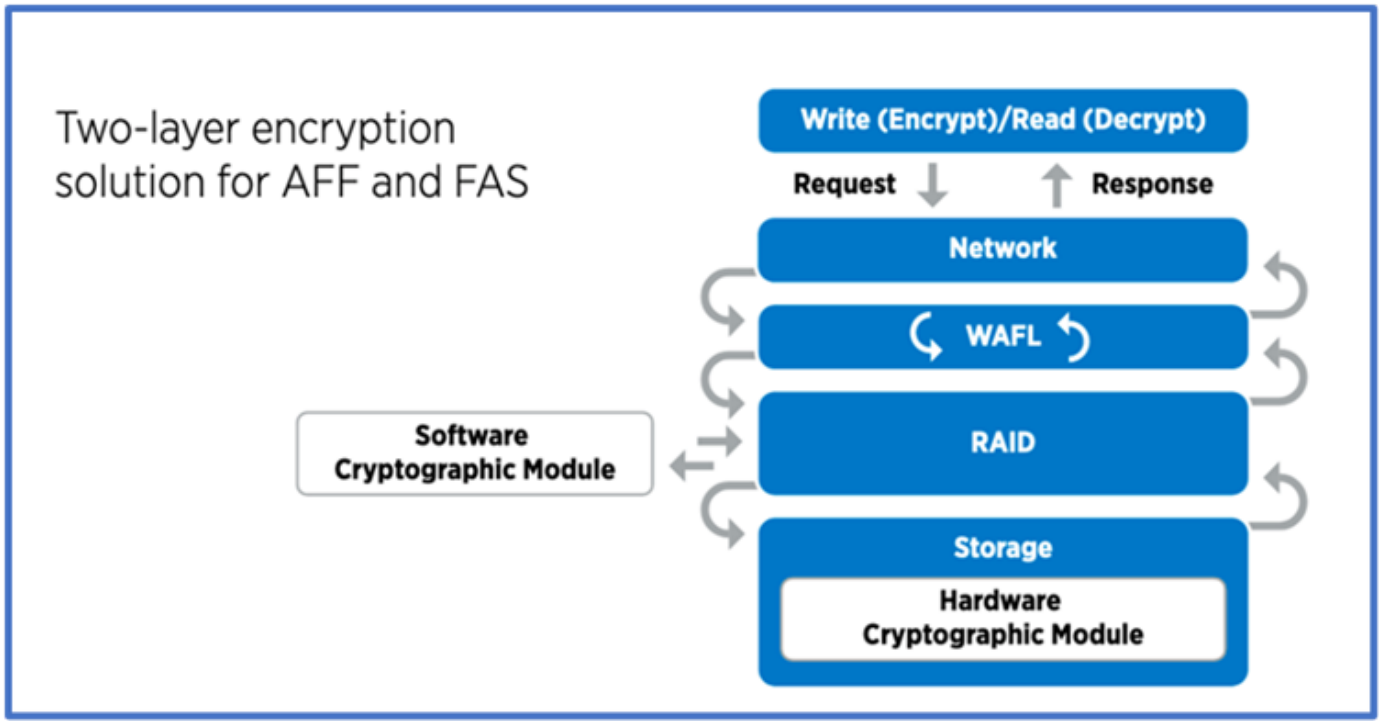
Uso de criptografia para dados em repouso e dados em trânsito

Criptografia de dados em repouso

Todos os dias, há novos requisitos para mitigar os riscos do sistema de storage e as lacunas de infraestrutura quando uma organização reutiliza unidades, retorna unidades com defeito ou atualiza "NetApp Storage Encryption (NSE) n.o 44; NetApp volume Encryption (NVE) n.o 44; e NetApp Aggregate Encryption" ajude você a criptografar todos os seus dados em repouso o tempo todo, seja tóxico ou não, sem afetar as operações diárias. "NSE" É uma solução de hardware ONTAP "dados em repouso"que utiliza unidades com autocriptografia validadas FIPS 140-2 nível 2. "NVE e NAE" São uma solução de software ONTAP "dados em repouso"que utiliza o "Módulo criptográfico NetApp validado FIPS 140-2 nível 1". Com NVE e NAE, os discos rígidos ou unidades de estado sólido podem ser usados para criptografia de dados em repouso. Além disso, as unidades NSE podem ser usadas para fornecer uma solução de criptografia nativa em camadas que fornece redundância de criptografia e segurança adicional. Se uma camada for violada, a segunda camada ainda protege os dados. Esses recursos tornam o ONTAP bem posicionado para "criptografia pronta para quantum"o .

O NVE também fornece uma funcionalidade chamada "purga segura" que remove criptograficamente dados tóxicos de derramamentos de dados quando arquivos confidenciais são gravados em um volume não classificado.

O "Gerenciador de chaves integrado (OKM)", que é o gerenciador de chaves integrado ao ONTAP, ou "aprovado" terceiros "gestores de chaves externos"podem ser usados com NSE e NVE para armazenar com segurança material de codificação.



Como visto na figura acima, a criptografia baseada em hardware e software pode ser combinada. Essa capacidade levou ao "Validação do ONTAP nas soluções comerciais da NSA para o programa classificado" que permite o armazenamento de dados secretos principais.

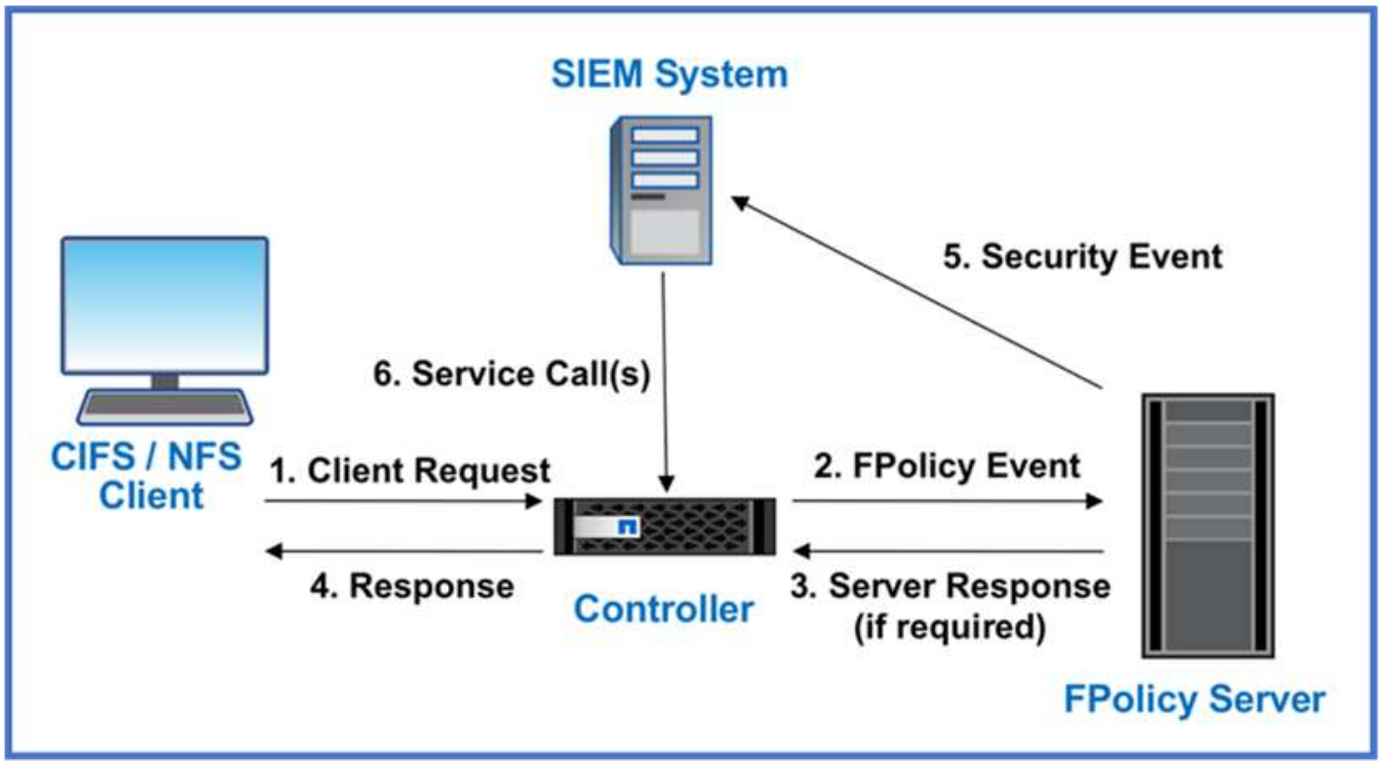
Criptografia de dados em trânsito

A criptografia de dados em trânsito do ONTAP protege o acesso aos dados do usuário e o acesso ao plano de controle. O acesso aos dados do usuário pode ser criptografado pela criptografia SMB 3,0 para o Microsoft CIFS Share Access ou pelo krb5P para NFS Kerberos 5. O acesso aos dados do usuário também pode ser criptografado com "IPsec"CIFS, NFS e iSCSI. O acesso ao plano de controle é criptografado com Transport Layer Security (TLS). O ONTAP fornece "FIPS"modo de conformidade para acesso ao plano de controle, o que habilita algoritmos aprovados pela FIPS e desabilita algoritmos que não são aprovados pela FIPS. A replicação de dados é criptografada com "criptografia por peer de cluster"o . Isso fornece criptografia para as tecnologias ONTAP SnapVault e SnapMirror.

Monitore e Registre todo o acesso

Depois que as políticas RBAC estiverem em vigor, você precisará implantar monitoramento, auditoria e alertas ativos. O mecanismo de confiança zero de FPolicy da NetApp ONTAP, juntamente com o "Ecossistema de parceiros do NetApp FPolicy", fornece os controles necessários para o modelo de confiança zero centrado em dados. O NetApp ONTAP é um software de gerenciamento de dados seguro e "FPolicy"é um recurso ONTAP líder do setor que oferece uma interface granular de notificação de eventos baseada em arquivo. Os parceiros do NetApp FPolicy podem usar essa interface para fornecer mais informações sobre o acesso aos dados no ONTAP. O recurso FPolicy do ONTAP, associado ao ecossistema de parceiros da Aliança NetApp dos parceiros FPolicy, permite identificar onde os dados da sua organização existem e quem tem acesso a eles. Isso é feito com análise comportamental do usuário, que identifica se os padrões de acesso aos dados são válidos. A análise comportamental do usuário pode ser usada para alertar para acesso a dados suspeitos ou aberrantes que estejam fora do padrão normal e, se necessário, tomar medidas para negar acesso.

Os parceiros do FPolicy estão indo além da análise comportamental do usuário em direção ao aprendizado de máquina (ML) e à inteligência artificial (AI) para maior fidelidade de eventos e menos, se houver, falsos positivos. Todos os eventos devem ser registrados em um servidor syslog ou em um sistema de gerenciamento de informações e eventos de segurança (SIEM) que também pode empregar ML e IA.



A Segurança de carga de trabalho de armazenamento da NetApp (anteriormente conhecida como "Cloud Secure") faz uso da interface FPolicy e da análise comportamental do usuário nos sistemas de storage ONTAP na nuvem e no local para fornecer alertas em tempo real sobre comportamento mal-intencionado do usuário. O Storage Workload Security protege os dados organizacionais contra a utilização indevida por usuários mal-intencionados ou comprometidos por meio do aprendizado de máquina avançado e da detecção de anomalias. O Storage Workload Security pode identificar ataques de ransomware ou outros comportamentos mal-intencionados, invocar cópias Snapshot e colocar em quarentena usuários mal-intencionados. O Storage Workload Security também tem uma capacidade forense para visualizar detalhadamente as atividades do usuário e da entidade. A segurança do workload de storage faz parte do NetApp Cloud Insights.

Além da segurança de workload de storage, o ONTAP tem uma funcionalidade de detecção de ransomware integrada conhecida como ARP (Onboard ransomware"Proteção autônoma contra ransomware"). O ARP usa aprendizado de máquina para determinar se uma atividade anormal de arquivos indica que um ataque de ransomware está em andamento e invoca uma cópia Snapshot e um alerta para os administradores. A segurança do workload de storage se integra ao ONTAP para receber eventos ARP e fornece uma camada adicional de análise e respostas automáticas.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Controles de orquestração e automação de segurança da NetApp externos ao ONTAP

A automação permite que você execute um processo ou procedimento com o mínimo de assistência humana. A automação permite que as organizações escalem implantações Zero Trust muito além dos procedimentos manuais para se defenderem de atividades maliciosas que também são automatizadas.

O Ansible é uma ferramenta de provisionamento de software de código aberto, gerenciamento de configurações e implantação de aplicações. Ele é executado em muitos sistemas Unix-like, e pode configurar

tanto sistemas Unix-like como Microsoft Windows. Ele inclui sua própria linguagem declarativa para descrever a configuração do sistema. Ansible foi escrito por Michael DeHaan e adquirido pela Red Hat em 2015. O Ansible está sem agente, conetando-se temporariamente remotamente por meio de SSH ou Gerenciamento remoto do Windows (permitindo a execução remota do PowerShell) para executar tarefas. O NetApp desenvolveu mais do que "150 módulos do Ansible para o software ONTAP"o , possibilitando ainda mais integração com a estrutura de automação do Ansible. Os módulos do Ansible para NetApp fornecem um conjunto de instruções para definir o estado desejado e reencaminhá-lo para o ambiente NetApp de destino. Os módulos são criados para dar suporte a tarefas como configuração de licenciamento, criação de agregados e máquinas virtuais de armazenamento, criação de volumes e restauração de instantâneos para citar alguns. Uma função do Ansible foi "Publicado no GitHub" específica do Guia de implantação de recursos unificados (UC) do NetApp DoD.

Usando a biblioteca de módulos disponíveis, os usuários podem facilmente desenvolver playbooks do Ansible e personalizá-los de acordo com suas próprias aplicações e necessidades empresariais para automatizar tarefas mundanas. Depois que um manual é escrito, você pode executá-lo para executar a tarefa especificada, o que economiza tempo e melhora a produtividade. A NetApp criou e compartilhou exemplos de playbooks que podem ser usados diretamente ou personalizados para suas necessidades.

O Cloud Insights é uma ferramenta de monitoramento de infraestrutura que oferece visibilidade de toda a sua infraestrutura. Com o Cloud Insights, você pode monitorar, solucionar problemas e otimizar todos os recursos, incluindo instâncias de nuvem pública e data centers privados. O Cloud Insights pode reduzir o tempo médio de resolução em 90% e impedir que 80% dos problemas de nuvem afetem os usuários finais. Ele também pode reduzir os custos de infraestrutura de nuvem em uma média de 33% e reduzir a exposição a ameaças internas protegendo seus dados com inteligência acionável. O recurso de segurança de carga de trabalho de armazenamento do Cloud Insights permite que análises comportamentais de usuários com IA e ML alertem quando comportamentos aberrantes de usuários ocorrem devido a uma ameaça interna. Para o ONTAP, a segurança da carga de trabalho de storage faz uso do mecanismo de FPolicy Zero Trust.

Implantações de nuvem híbrida e de confiança zero

A NetApp é a autoridade em dados para a nuvem híbrida. O NetApp oferece várias opções para estender os sistemas de gerenciamento de dados locais para a nuvem híbrida com o Amazon Web Services (AWS), o Microsoft Azure, o Google Cloud Platform (GCP) e outros fornecedores de nuvem líderes do setor. As soluções de nuvem híbrida da NetApp são compatíveis com os mesmos controles de segurança Zero Trust que estão disponíveis nos sistemas ONTAP no local e no storage definido por software da ONTAP Select.

Amplie a capacidade em nuvens públicas com facilidade sem restrições de capex típicas usando o NetApp Cloud Volumes Service, o primeiro serviço de arquivos nativo em nuvem de classe empresarial para AWS e GCP e o Azure NetApp Files para Microsoft Azure. Ideal para workloads com uso intenso de dados, como análises e DevOps, esses serviços de dados em nuvem combinam storage elástico sob demanda como serviço da NetApp com o gerenciamento de dados da ONTAP em uma oferta totalmente gerenciada.

Para aqueles que buscam serviços avançados de dados para serviços de storage de objetos ou bloco na nuvem, como AWS EBS e S3 ou Azure Storage, o Cloud Volumes ONTAP oferece gerenciamento de dados entre seu ambiente local e a nuvem pública com uma única visualização comum. Executado na AWS ou no Azure como uma instância sob demanda, o Cloud Volumes ONTAP fornece a eficiência de storage, a disponibilidade e a escalabilidade do software ONTAP. O ONTAP permite a movimentação de dados entre os sistemas ONTAP no local e o ambiente de storage da AWS ou do Azure com o software de replicação de dados NetApp SnapMirror.

Proteção de dados e recuperação de desastres

Peering de cluster e SVM

Visão geral do peering de cluster e SVM

Você pode criar relacionamentos entre clusters de origem e destino e entre máquinas virtuais de armazenamento de origem e destino (SVMs). Você precisa criar relacionamentos entre pares entre essas entidades antes de poder replicar cópias Snapshot usando o SnapMirror.

O ONTAP 9.3 oferece aprimoramentos que simplificam a maneira como você configura relacionamentos entre clusters e SVMs. Os procedimentos de peering de cluster e SVMs estão disponíveis para todas as versões do ONTAP 9. Você deve usar o procedimento apropriado para sua versão do ONTAP.

Você executa os procedimentos usando a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Preparar-se para peering de cluster e SVM

Noções básicas de peering

Você deve criar relacionamentos *peer* entre clusters de origem e destino e entre SVMs de origem e destino antes de poder replicar cópias Snapshot usando o SnapMirror. Um relacionamento de pares define conexões de rede que permitem que clusters e SVMs troquem dados com segurança.

Clusters e SVMs em relações entre pares se comunicam pela rede entre clusters usando *interfaces lógicas (LIFs).* um LIF entre clusters é um LIF que suporta o serviço de interface de rede "entre clusters-core" e é normalmente criado usando a política de serviço de interface de rede "default-clusters". É necessário criar LIFs entre clusters em cada nó nos clusters que estão sendo perados.

Os LIFs usam rotas que pertencem ao SVM do sistema ao qual são atribuídos. O ONTAP cria automaticamente um sistema SVM para comunicações em nível de cluster em um espaço de IPspace.

Topologias de fan-out e cascata são suportadas. Em uma topologia em cascata, você só precisa criar redes entre clusters primários e secundários e entre clusters secundários e secundários. Não é necessário criar uma rede entre clusters primário e terciário.

> É possível (mas não aconselhável) que um administrador remova o serviço entre clusters da política de serviços padrão entre clusters. Se isso ocorrer, LIFs criadas usando "default-clusters" não serão, na verdade, LIFs entre clusters. Para confirmar que a política de serviço padrão contém o serviço entre clusters-core, use o seguinte comando:
>
> ```
> network interface service-policy show -policy default-intercluster
> ```

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar se os requisitos de conetividade, porta, endereço IP, sub-rede, firewall e nomenclatura de cluster são

atendidos.

> A partir do ONTAP 9.6, o peering de cluster fornece suporte de criptografia TLS 1,2 AES-256 GCM para replicação de dados por padrão. As cifras de segurança padrão ("PSK-AES256-GCM-SHA384") são necessárias para que o peering de cluster funcione mesmo que a criptografia esteja desativada.
>
> Começando com ONTAP 9.11,1, as cifras de segurança DHE-PSK estão disponíveis por padrão.
>
> A partir do ONTAP 9.15,1, o peering de cluster fornece suporte de criptografia TLS 1,3 para replicação de dados por padrão.

Requisitos de conetividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve pertencer ao domínio de broadcast que contém as portas usadas para comunicação entre clusters.
- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

  Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.

> O ONTAP permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

  Você pode usar vários IPspaces para fazer pares com vários clusters. A conetividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

  As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de

interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall

A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Tráfego ICMP bidirecional
- Tráfego TCP iniciado bidirecional para os endereços IP de todas as LIFs entre clusters nas portas 11104 e 11105
- HTTPS bidirecional entre os LIFs entre clusters

  Embora o HTTPS não seja necessário quando você configura o peering de cluster usando a CLI, o HTTPS é necessário mais tarde se você usar o System Manager para configurar a proteção de dados.

A política de firewall predefinida `intercluster` permite o acesso através do protocolo HTTPS e de todos os endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Requisito de cluster

Os clusters precisam atender aos seguintes requisitos:

- Um cluster não pode estar em um relacionamento de pares com mais de 255 clusters.

Use portas compartilhadas ou dedicadas

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. Ao decidir se deseja compartilhar portas, você precisa considerar a largura de banda da rede, o intervalo de replicação e a disponibilidade da porta.

Você pode compartilhar portas em um cluster com peered enquanto usa portas dedicadas no outro.

Largura de banda da rede

Se você tiver uma rede de alta velocidade, como 10 GbE, talvez tenha largura de banda local suficiente para executar a replicação usando as mesmas portas de 10 GbE usadas para acesso aos dados.

Mesmo assim, você deve comparar a largura de banda da WAN disponível com a largura de banda da LAN. Se a largura de banda da WAN disponível for significativamente menor que 10 GbE, talvez seja necessário usar portas dedicadas.

A única exceção a essa regra pode ser quando todos ou muitos nós no cluster replicarem dados, caso em que a utilização da largura de banda é normalmente espalhada pelos nós.

Se você não estiver usando portas dedicadas, o tamanho máximo da unidade de transmissão (MTU) da rede de replicação geralmente deve ser o mesmo que o tamanho da MTU da rede de dados.

Intervalo de replicação

Se a replicação ocorrer em horas fora do pico, você poderá usar portas de dados para replicação mesmo sem uma conexão LAN de 10 GbE.

Se a replicação ocorrer durante o horário comercial normal, você precisa considerar a quantidade de dados que serão replicados e se ela precisará de tanta largura de banda que poderia causar contenção com protocolos de dados. Se a utilização da rede por protocolos de dados (SMB, NFS, iSCSI) for superior a 50%, deverá utilizar portas dedicadas para comunicação entre clusters, para permitir uma performance não degradada se ocorrer failover de nó.

Disponibilidade da porta

Se você determinar que o tráfego de replicação está interferindo no tráfego de dados, poderá migrar LIFs para qualquer outra porta compartilhada com capacidade para clusters no mesmo nó.

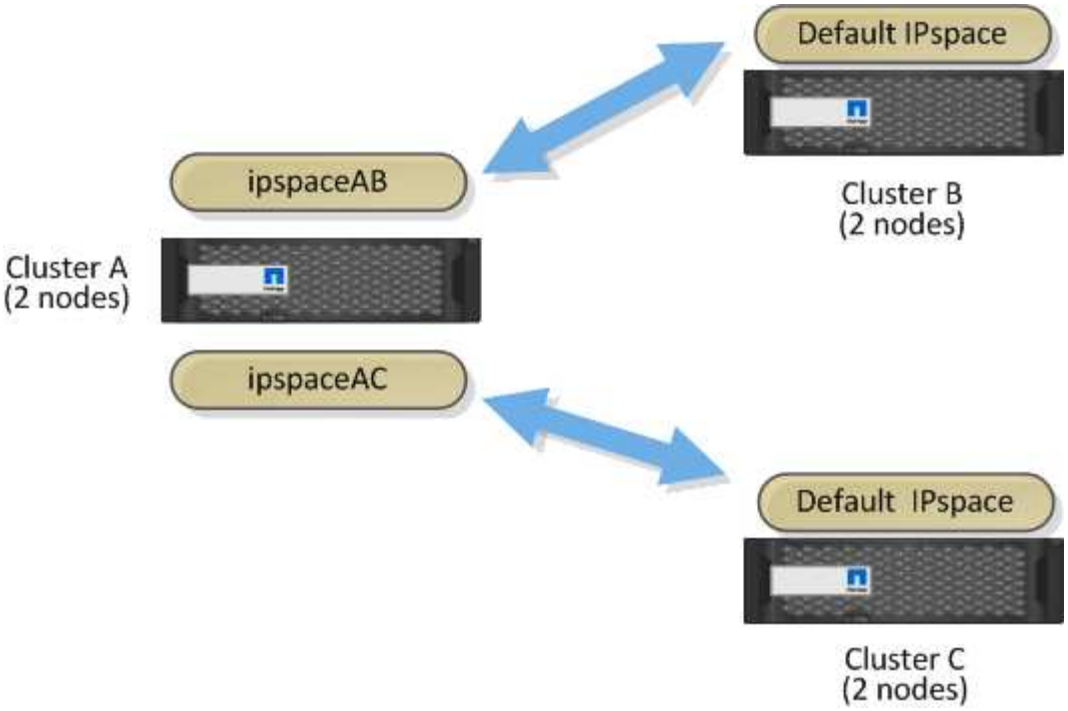
Você também pode dedicar portas VLAN para replicação. A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

Use IPspaces personalizados para isolar o tráfego de replicação

Você pode usar IPspaces personalizados para separar as interações que um cluster tem com seus pares. Chamada de *conetividade entre clusters designada*, essa configuração permite que os provedores de serviços isolem o tráfego de replicação em ambientes multitenant.

Suponha, por exemplo, que você deseja que o tráfego de replicação entre o Cluster A e o Cluster B seja separado do tráfego de replicação entre o Cluster A e o Cluster C. para conseguir isso, você pode criar dois espaços IPspaces no Cluster A.

Um IPspace contém as LIFs entre clusters que você usa para se comunicar com o Cluster B. o outro contém as LIFs entre clusters que você usa para se comunicar com o Cluster C, como mostrado na ilustração a seguir.



Para a configuração de IPspace personalizada, consulte o *Network Management Guide*.

Configurar LIFs entre clusters

Configurar LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Passos

1. Liste as portas no cluster:

   ```
   network port show
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Crie LIFs entre clusters em um administrador SVM (IPspace padrão) ou em um sistema SVM (IPspace personalizado):

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
Em ONTAP 9.5 e anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` na `e0c` porta irão falhar para a `e0d` porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Configurar LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que portas `e0e` e `e0f` não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Crie um grupo de failover para as portas dedicadas:

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

O exemplo a seguir atribui portas `e0e` e `e0f` ao grupo de failover `intercluster01` no SVM do sistema `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verifique se o grupo de failover foi criado:

`network interface failover-groups show`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`

Opção	Descrição
Em ONTAP 9.5 e anteriores:	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` no grupo failover `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` a porta SVM`e0e` farão failover para a `e0f` porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar LIFs entre clusters em IPspaces personalizados

Você pode configurar LIFs entre clusters em IPspaces personalizados. Isso permite isolar o tráfego de replicação em ambientes multitenant.

Quando você cria um IPspace personalizado, o sistema cria uma máquina virtual de storage do sistema (SVM) para servir como um contêiner para os objetos do sistema nesse IPspace. Você pode usar o novo SVM como contêiner para quaisquer LIFs entre clusters no novo IPspace. O novo SVM tem o mesmo nome que o IPspace personalizado.

Passos

1. Liste as portas no cluster:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as portas de rede no `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Crie IPspaces personalizados no cluster:

   `network ipspace create -ipspace` *`ipspace`*

   O exemplo a seguir cria o IPspace personalizado `ipspace-IC1` :

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

3. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

   `network interface show -fields home-port,curr-port`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que portas `e0e` e `e0f` não foram atribuídas LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. Remova as portas disponíveis do domínio de broadcast padrão:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Uma porta não pode estar em mais de um domínio de broadcast de cada vez. Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir remove portas `e0e` e `e0f` do domínio de broadcast padrão:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Verifique se as portas foram removidas do domínio de broadcast padrão:

   `network port show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que as portas `e0e` e `e0f` foram removidas do domínio de broadcast padrão:

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Crie um domínio de broadcast no IPspace personalizado:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   O exemplo a seguir cria o domínio de broadcast `ipspace-IC1-bd` no IPspace : `ipspace-IC1`

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Verifique se o domínio de broadcast foi criado:

   `network port broadcast-domain show`

   Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  ---------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a             complete
                            cluster01-01:e0b             complete
                            cluster01-02:e0a             complete
                            cluster01-02:e0b             complete
Default Default       1500
                            cluster01-01:e0c             complete
                            cluster01-01:e0d             complete
                            cluster01-01:e0f             complete
                            cluster01-01:e0g             complete
                            cluster01-02:e0c             complete
                            cluster01-02:e0d             complete
                            cluster01-02:e0f             complete
                            cluster01-02:e0g             complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e             complete
                            cluster01-01:e0f             complete
                            cluster01-02:e0e             complete
                            cluster01-02:e0f             complete
```

8. Crie LIFs entre clusters no sistema SVM e atribua-os ao domínio de broadcast:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
Em ONTAP 9.5 e anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

O LIF é criado no domínio de broadcast ao qual a porta inicial é atribuída. O domínio de broadcast tem um grupo de failover padrão com o mesmo nome do domínio de broadcast. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` no domínio de broadcast `ipspace-IC1-bd` :

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster`

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	`network interface show -service-policy default-intercluster -failover`
Em ONTAP 9.5 e anteriores:	`network interface show -role intercluster -failover`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` a porta SVM `e0e` fazem failover para a porta 'e0f':

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar relações entre pares

Crie um relacionamento de pares de cluster

Antes de proteger seus dados replicando-os em um cluster remoto para fins de backup de dados e recuperação de desastres, você deve criar um relacionamento de peers de clusters entre o cluster local e o cluster remoto.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar a replicação de snapshot de configuração. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Várias políticas de proteção padrão estão disponíveis. Você deve ter criado suas políticas de proteção se quiser usar políticas personalizadas.

Antes de começar

- Se você estiver usando a CLI do ONTAP, crie LIFs entre clusters em todos os nós dos clusters que estão sendo direcionados usando um dos seguintes métodos:

    - "Configurar LIFs entre clusters em portas de dados compartilhados"
    - "Configurar LIFs entre clusters em portas de dados dedicadas"
    - "Configurar LIFs entre clusters em IPspaces personalizados"
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior. (Se os clusters estiverem executando o ONTAP 9.2 ou anterior, consulte os procedimentos em "este documento arquivado".)

Passos

Execute esta tarefa usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

1. No cluster local, clique em **Cluster > Settings**.
2. Na seção **Configurações de cluster**, clique em **Adicionar interfaces de rede** e insira o endereço IP e a máscara de sub-rede para adicionar interfaces de rede entre clusters para o cluster.

   Repita este passo no painel remoto.
3. No cluster remoto, clique em **Cluster > Settings**.
4. Clique ⋮ na secção **Cluster Peers** e selecione **Generate Passphrase** (gerar frase-passe).
5. Selecione a versão remota do cluster do ONTAP.
6. Copie a frase-passe gerada.
7. No cluster local, em **Cluster Peers**, clique ⋮ e selecione **Peer cluster**.
8. Na janela **cluster de pares**, cole a frase-passe e clique em **Iniciar peering de cluster**.

CLI

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   Se você especificar ambos `-generate-passphrase` e `-peer-addrs`, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addrs` poderá usar a senha gerada.

   Você pode ignorar a `-ipspace` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

   Se você estiver criando o relacionamento de peering no ONTAP 9.6 ou posterior e não quiser que as comunicações de peering entre clusters sejam criptografadas, use a `-encryption-protocol -proposed none` opção para desativar a criptografia.

   O exemplo a seguir cria um relacionamento de peer de cluster com um cluster remoto não especificado e pré-autoriza relacionamentos entre pares com SVMs e `vs1` `vs2` no cluster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

O exemplo a seguir cria um relacionamento de peer de cluster com o cluster remoto nos endereços IP de LIF 192.140.112.103 e 192.140.112.104 e pré-autoriza um relacionamento de pares com qualquer SVM no cluster local:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

O exemplo a seguir cria um relacionamento de peer de cluster com um cluster remoto não especificado e pré-autoriza relacionamentos entre pares com SVMs e`vs1` `vs2` no cluster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. No cluster de origem, autentique o cluster de origem no cluster de destino:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir autentica o cluster local para o cluster remoto nos endereços IP 192.140.112.101 e 192.140.112.102 do LIF:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                   Address Family of Relationship: ipv4
               Authentication Status Administrative: no-authentication
                  Authentication Status Operational: absent
                                Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. Verifique a conetividade e o status dos nós no relacionamento de pares:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da preparação para recuperação de desastres em volume"

Criar um relacionamento entre pares SVM entre clusters

Você pode usar o `vserver peer create` comando para criar um relacionamento entre SVMs em clusters locais e remotos.

Antes de começar

- Os clusters de origem e destino devem ser percorridos.
- Os clusters devem estar executando o ONTAP 9.3. (Se os clusters estiverem executando o ONTAP 9.2 ou

anterior, consulte os procedimentos em "este documento arquivado".)

- Você deve ter relações de pares "pré-autorizadas" para os SVMs no cluster remoto.

  Para obter mais informações, "Criando um relacionamento de cluster peer"consulte .

Sobre esta tarefa

No ONTAP 9.2 e anteriores, você pode autorizar um relacionamento de pares para apenas um SVM de cada vez. Isso significa que você precisa executar o `vserver peer accept` comando cada vez que você autorizar um relacionamento de pares SVM pendente.

A partir do ONTAP 9.3, você pode "pré-autorizar" relacionamentos de pares para vários SVMs, listando os SVMs na `-initial-allowed-vserver` opção quando você cria um relacionamento de peer de cluster. Para obter mais informações, "Criando um relacionamento de cluster peer"consulte .

Passos

1. No cluster de destino de proteção de dados, exiba os SVMs que são pré-autorizados para peering:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. No cluster de origem de proteção de dados, crie um relacionamento de mesmo nível com um SVM pré-autorizado no cluster de destino de proteção de dados:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um relacionamento entre o SVM local `pvs1` e o SVM remoto pré-autorizado `vs1` :

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Verifique o relacionamento entre pares SVM:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Adicione um relacionamento entre pares SVM entre clusters

Se você criar um SVM depois de configurar um relacionamento de pares de cluster, precisará adicionar um relacionamento de mesmo nível para o SVM manualmente. Você pode usar o `vserver peer create` comando para criar um relacionamento entre pares entre SVMs. Após a criação do relacionamento de pares, você pode executar `vserver peer accept` no cluster remoto para autorizar o relacionamento de pares.

Antes de começar

Os clusters de origem e destino devem ser percorridos.

Sobre esta tarefa

Você pode criar relacionamentos entre pares entre SVMs no mesmo cluster para backup de dados locais. Para obter mais informações, consulte a `vserver peer create` página de manual.

Os administradores ocasionalmente usam o `vserver peer reject` comando para rejeitar uma proposta de relacionamento com colegas SVM. Se a relação entre SVMs estiver no `rejected` estado, você deverá excluir a relação antes de criar uma nova. Para obter mais informações, consulte a `vserver peer delete` página de manual.

Passos

1. No cluster de origem de proteção de dados, crie um relacionamento de mesmo nível com um SVM no cluster de destino de proteção de dados:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   O exemplo a seguir cria um relacionamento entre o SVM local`pvs1` e o SVM remoto`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Se os SVMs locais e remotos tiverem os mesmos nomes, você deverá usar um *local name* para criar o relacionamento de pares SVM:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. No cluster de origem de proteção de dados, verifique se o relacionamento de pares foi iniciado:

   `vserver peer show-all`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra que a relação entre SVM`pvs1` e SVM`vs1` foi iniciada:

```
cluster01::> vserver peer show-all
            Peer        Peer                        Peering
Vserver     Vserver     State      Peer Cluster     Applications
--------    --------    ---------  -------------    ------------
pvs1        vs1         initiated   Cluster02         snapmirror
```

3. No cluster de destino da proteção de dados, exiba a relação de pares SVM pendente:

   `vserver peer show`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir lista as relações de pares pendentes para `cluster02`:

```
cluster02::> vserver peer show

                  Peer               Peer
Vserver           Vserver            State
-----------       -----------        ------------
vs1               pvs1               pending
```

4. No cluster de destino de proteção de dados, autorize o relacionamento de pares pendente:

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir autoriza o relacionamento entre pares entre o SVM local `vs1` e o SVM remoto `pvs1` :

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Verifique o relacionamento entre pares SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Habilitar a criptografia de peering de cluster em um relacionamento de pares existente

A partir do ONTAP 9.6, a criptografia de peering de cluster é ativada por padrão em todas as relações de peering de cluster recém-criadas. A criptografia de peering de cluster usa uma chave pré-compartilhada (PSK) e a camada de segurança de transporte (TLS) para proteger as comunicações de peering entre clusters. Isso adiciona uma camada adicional de segurança entre os clusters com peering.

Sobre esta tarefa

Se você estiver atualizando clusters peered para o ONTAP 9.6 ou posterior e a relação de peering tiver sido criada no ONTAP 9.5 ou anterior, a criptografia de peering de cluster deve ser ativada manualmente após a atualização. Ambos os clusters no relacionamento de peering devem estar executando o ONTAP 9.6 ou posterior para habilitar a criptografia de peering de cluster.

Passos

1. No cluster de destino, ative a encriptação para comunicações com o cluster de origem:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Quando solicitado, introduza uma frase-passe.
3. No cluster de origem da proteção de dados, ative a criptografia para comunicação com o cluster de destino da proteção de dados:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Quando solicitado, introduza a mesma frase-passe introduzida no cluster de destino.

Remova a criptografia de peering de cluster de um relacionamento de pares existente

Por padrão, a criptografia de peering de cluster é ativada em todos os relacionamentos de pares criados no ONTAP 9.6 ou posterior. Se você não quiser usar criptografia para

comunicações de peering entre clusters, você pode desativá-la.

Passos

1. No cluster de destino, modifique as comunicações com o cluster de origem para interromper o uso da criptografia de peering de cluster:
   - Para remover a criptografia, mas manter a autenticação, digite:

     ```
     cluster peer modify <source_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para remover criptografia e autenticação:
     i. Modifique a política de peering de cluster para permitir acesso não autenticado:

     ```
     cluster peer policy modify -is-unauthenticated-access-permitted
     true
     ```

     ii. Modificar criptografia e acesso de autenticação:

     ```
     cluster peer modify <source_cluster> -auth-status no-
     authentication
     ```

2. Quando solicitado, introduza a frase-passe.
3. Confirme a frase-passe reinserindo-a.
4. No cluster de origem, desative a encriptação para comunicação com o cluster de destino:
   - Para remover a criptografia, mas manter a autenticação, digite:

     ```
     cluster peer modify <destination_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para remover criptografia e autenticação:
     i. Modifique a política de peering de cluster para permitir acesso não autenticado:

     ```
     cluster peer policy modify -is-unauthenticated-access-permitted
     true
     ```

     ii. Modificar criptografia e acesso de autenticação:

     ```
     cluster peer modify <destination_cluster> -auth-status no-
     authentication
     ```

5. Quando solicitado, introduza e introduza novamente a mesma frase-passe utilizada no cluster de destino.

Gerenciar snapshots locais

Visão geral do gerenciamento de cópias Snapshot locais

Uma *cópia Snapshot* é uma imagem pontual e somente leitura de um volume. A imagem consome espaço de armazenamento mínimo e incorre em sobrecarga de desempenho insignificante, pois Registra apenas alterações nos arquivos desde a última cópia Snapshot.

Você pode usar uma cópia Snapshot para restaurar todo o conteúdo de um volume ou para recuperar arquivos individuais ou LUNs. As cópias snapshot são armazenadas no diretório `.snapshot` do volume.

No ONTAP 9.3 e versões anteriores, um volume pode conter até 255 cópias Snapshot. No ONTAP 9.4 e posterior, um FlexVol volume pode conter até 1023 cópias snapshot.

A partir do ONTAP 9.8, os volumes FlexGroup podem conter 1023 cópias Snapshot. Para obter mais informações, "Proteja volumes FlexGroup com cópias Snapshot"consulte .

Configurar políticas de snapshot personalizadas

Configurar uma visão geral das políticas de Snapshot personalizadas

Uma política *Snapshot* define como o sistema cria cópias Snapshot. A política especifica quando criar cópias Snapshot, quantas cópias devem ser mantidas e como nomeá-las. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes e nomear as cópias "diárias.`*timestamp*`".

A política padrão de um volume cria automaticamente cópias Snapshot na programação a seguir, com as cópias Snapshot mais antigas excluídas para abrir espaço para cópias mais recentes:

- Um máximo de seis cópias Snapshot por hora levou cinco minutos depois da hora.
- Um máximo de duas cópias snapshot diárias realizadas de segunda a sábado, 10 minutos após a meia-noite.
- Um máximo de duas cópias Snapshot semanais realizadas todos os domingos, aos 15 minutos após a meia-noite.

A menos que você especifique uma política de Snapshot ao criar um volume, o volume herda a política de Snapshot associada a ela que contém a máquina virtual de storage (SVM).

Quando configurar uma política Snapshot personalizada

Se a política Snapshot padrão não for apropriada para um volume, você poderá configurar uma política personalizada que modifique a frequência, a retenção e o nome das cópias snapshot. A programação será ditada principalmente pela taxa de alteração do sistema de arquivos ativo.

Você pode fazer backup de um sistema de arquivos muito usado como um banco de dados a cada hora,

enquanto você faz backup de arquivos raramente usados uma vez por dia. Mesmo para um banco de dados, você normalmente executa um backup completo uma ou duas vezes por dia, enquanto faz backup de logs de transações a cada hora.

Outros fatores são a importância dos arquivos para a sua organização, seu Contrato de nível de Serviço (SLA), seu objetivo do ponto de recuperação (RPO) e seu objetivo de tempo de recuperação (rto). De um modo geral, você deve reter apenas quantas cópias snapshot forem necessárias.

Criar um agendamento de trabalho instantâneo

Uma política Snapshot requer pelo menos um agendamento de trabalho de cópia Snapshot. Você pode usar o System Manager ou o `job schedule cron create` comando para criar uma agenda de tarefas.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar uma agenda de trabalhos instantâneos. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Por padrão, o ONTAP forma os nomes das cópias Snapshot anexando um carimbo de data/hora ao nome da programação de trabalhos.

Se você especificar valores para o dia do mês e o dia da semana, os valores serão considerados independentemente. Por exemplo, um cronograma do cron com a especificação do dia `Friday` e a especificação do dia do mês `13` é executado todas as sextas-feiras e no dia 13th de cada mês, não apenas em todas as sextas-feiras, dia 13th.

Exemplo 27. Passos

System Manager

1. Navegue até **proteção > Visão geral** e expanda **configurações de política local**.
2. No painel **horários**, clique em .
3. Na janela **horários**, clique Add em .
4. Na janela **Adicionar agendamento**, insira o nome da programação e escolha o contexto e o tipo de agendamento.
5. Clique em **Salvar**.

CLI

1. Criar uma agenda de trabalhos:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

A partir do ONTAP 9.10,1, você pode incluir o SVM para sua agenda de trabalho:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

O exemplo a seguir cria um horário de trabalho chamado `myweekly` que é executado aos sábados às 3:00 da manhã:

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

O exemplo a seguir cria uma programação chamada `myweeklymulti` que especifica vários dias, horas e minutos:

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

Criar uma política Snapshot

Uma política Snapshot especifica quando criar cópias Snapshot, quantas cópias devem ser mantidas e como nomeá-las. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes e

nomeá-las "diárias.`*timestamp*`". Uma política Snapshot pode conter até cinco agendamentos de tarefas.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar uma política de snapshot. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Por padrão, o ONTAP forma os nomes das cópias Snapshot anexando um carimbo de data/hora ao nome da programação de trabalhos:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Se preferir, pode substituir um prefixo para o nome da agenda de trabalhos.

A `snapmirror-label` opção é para replicação SnapMirror. Para obter mais informações, "Definir uma regra para uma política"consulte .

Passos

Você pode criar uma política de cópia Snapshot usando o Gerenciador do sistema ou a CLI do ONTAP. O procedimento cria uma política de cópia Snapshot apenas no cluster local.

System Manager

1. Navegue até **proteção > Visão geral** e expanda **configurações de política local**.
2. No painel **políticas de instantâneos**, clique em .
3. Na guia **políticas de instantâneos**, clique Add em .
4. Na janela **Add Snapshot policy** (Adicionar instantâneo), insira o nome da política e escolha o escopo.
5. Clique Add em .
6. Para selecionar uma programação, clique no nome da programação atualmente exibida, clique em e escolha uma programação diferente.
7. Insira o máximo de cópias Snapshot a reter e, se necessário, insira o rótulo SnapMirror e o período de retenção do SnapLock.
8. Clique em **Salvar**.

CLI

1. Criar uma política Snapshot:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

O exemplo a seguir cria uma política de Snapshot chamada `snap_policy_daily` que é executada em um `daily` agendamento. A política tem no máximo cinco cópias Snapshot, cada uma com o nome `daily.`*`timestamp`* e o rótulo SnapMirror `daily` :

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

Gerencie cópias Snapshot manualmente

Criar e excluir cópias Snapshot manualmente

Você pode criar cópias Snapshot manualmente quando não puder esperar que uma cópia Snapshot agendada seja criada. Além disso, você pode excluir cópias snapshot quando elas não forem mais necessárias.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar um snapshot sob demanda. Os sistemas ASA R2

fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Crie uma cópia Snapshot manualmente

Você pode criar manualmente uma cópia Snapshot usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

Passos

1. Navegue até **armazenamento > volumes** e selecione a guia **cópias Snapshot**.
2. Clique + Add em .
3. Na janela **Adicionar uma cópia Snapshot**, aceite o nome da cópia Snapshot padrão ou edite-o, se desejado.
4. **Opcional**: Adicione uma etiqueta SnapMirror.
5. Clique em **Add**.

CLI

1. Criar uma cópia Snapshot:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Exclua uma cópia Snapshot manualmente

Você pode excluir manualmente uma cópia Snapshot usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

Passos

1. Navegue até **armazenamento > volumes** e selecione a guia **cópias Snapshot**.
2. Localize a cópia Snapshot que deseja excluir, clique ⋮ em e selecione **Excluir**.
3. Na janela **Excluir cópia Snapshot**, selecione **Excluir cópia Snapshot**.
4. Clique em **Excluir**.

CLI

1. Excluir uma cópia Snapshot:

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Calcule o espaço que pode ser recuperado antes de excluir cópias Snapshot

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para selecionar

cópias Snapshot que deseja excluir e calcular o espaço que pode ser recuperado antes de excluí-las.

Passos

1. Clique em **armazenamento > volumes**.
2. Selecione o volume a partir do qual deseja excluir cópias Snapshot.
3. Clique em **cópias Snapshot**.
4. Selecione uma ou mais cópias Snapshot.
5. Clique em **Calculate Recenclaable Space** (calcular espaço de recuperação).

Gerenciar a reserva de cópias Snapshot

Gerencie a visão geral da reserva de cópias instantâneas

O *reserva de cópia Snapshot* reserva uma porcentagem de espaço em disco para cópias Snapshot, cinco por padrão. Como as cópias Snapshot usam espaço no sistema de arquivos ativo quando a reserva de cópias Snapshot está esgotada, talvez você queira aumentar a reserva de cópias snapshot conforme necessário. Como alternativa, você pode fazer cópias Snapshot autodelete quando a reserva estiver cheia.

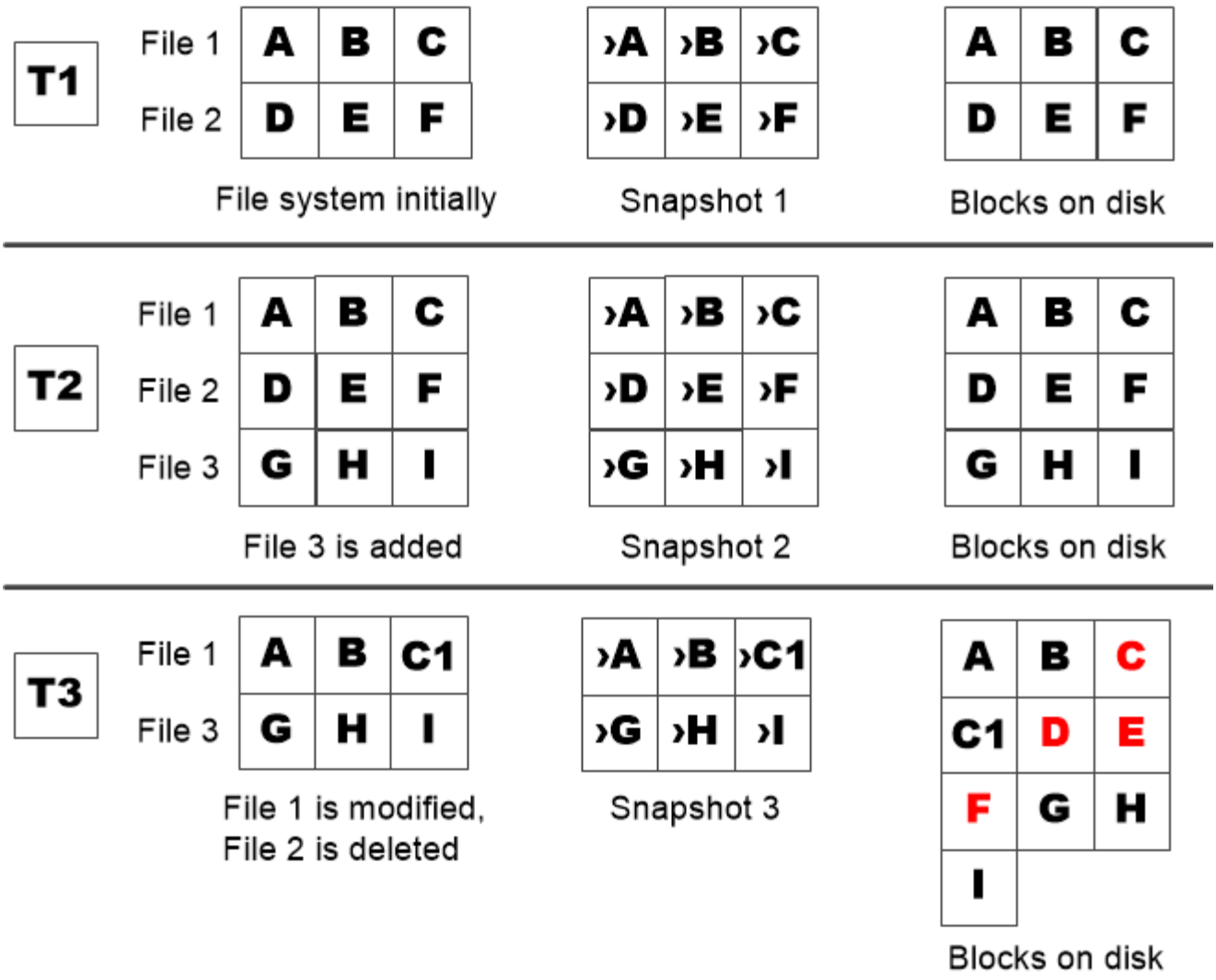
Quando aumentar a reserva de cópia Snapshot

Ao decidir se deseja aumentar a reserva Snapshot, é importante lembrar que uma cópia Snapshot Registra apenas alterações nos arquivos desde que a última cópia Snapshot foi feita. Ele consome espaço em disco somente quando blocos no sistema de arquivos ativo são modificados ou excluídos.

Isso significa que a taxa de alteração do sistema de arquivos é o fator chave para determinar a quantidade de espaço em disco usada pelas cópias Snapshot. Não importa quantas cópias Snapshot você criar, elas não consumirão espaço em disco se o sistema de arquivos ativo não for alterado.

Um FlexVol volume contendo logs de transação de banco de dados, por exemplo, pode ter uma reserva de cópia Snapshot tão grande quanto 20% para contabilizar sua maior taxa de alteração. Não só você deseja criar mais cópias Snapshot para capturar as atualizações mais frequentes do banco de dados, como também ter uma reserva de cópias Snapshot maior para lidar com o espaço de disco adicional que as cópias snapshot consomem.

Uma cópia Snapshot consiste em ponteiros para blocos em vez de cópias de blocos. Você pode pensar em um ponteiro como uma "reivindicação" em um bloco: O ONTAP mantém o bloco até que a cópia Snapshot seja excluída.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

Como excluir arquivos protegidos pode levar a menos espaço do arquivo do que o esperado

Uma cópia Snapshot aponta para um bloco mesmo depois que você exclui o arquivo que usou o bloco. Isso explica por que uma reserva de cópia Snapshot esgotada pode levar ao resultado contra-intuitivo no qual a exclusão de um sistema de arquivos inteiro resulta em menos espaço disponível do que o sistema de arquivos ocupado.

Considere o exemplo a seguir. Antes de excluir quaisquer arquivos, a `df` saída do comando é a seguinte:

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Depois de excluir todo o sistema de arquivos e fazer uma cópia Snapshot do volume, o `df` comando gera a seguinte saída:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Como mostra a saída, os 3 GB usados anteriormente pelo sistema de arquivos ativo agora estão sendo usados por cópias Snapshot, além dos 0,5 GB usados antes da exclusão.

Como o espaço em disco usado pelas cópias Snapshot agora excede a reserva de cópias Snapshot, o excesso de 2,5 GB "pílulas" para o espaço reservado para arquivos ativos, deixando você com 0,5 GB de espaço livre para arquivos onde você poderia razoavelmente ter esperado 3 GB.

Monitorar o consumo do disco de cópia Snapshot

Você pode monitorar o consumo de disco de cópia Snapshot usando o `df` comando. O comando exibe a quantidade de espaço livre no sistema de arquivos ativo e na reserva de cópia Snapshot.

Passo

1. Exibir consumo do disco de cópia Snapshot: `df`

   O exemplo a seguir mostra o consumo do disco de cópia Snapshot:

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Verifique a reserva de cópias Snapshot disponível em um volume

Você pode querer verificar quanto reserva de cópia Snapshot está disponível em um volume usando o `snapshot-reserve-available` parâmetro com o `volume show` comando.

Passo

1. Verifique a reserva de cópias instantâneas disponível em um volume:

   `vol show -vserver` *`SVM`* `-volume` *`volume`* `-fields snapshot-reserve-available`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir exibe a reserva de cópia Snapshot disponível para `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

Modifique a reserva de cópia Snapshot

Talvez você queira configurar uma reserva de cópias Snapshot maior para impedir que cópias snapshot usem espaço reservado para o sistema de arquivos ativo. Você pode diminuir a reserva de cópias Snapshot quando não precisar mais de espaço para cópias Snapshot.

Passo

1. Modificar a reserva de cópia Instantânea:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-percent-snapshot-space` *`snap_reserve`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir define a reserva de cópia Snapshot para `vol1` 10%:

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

Cópias Snapshot Autodelete

Você pode usar o `volume snapshot autodelete modify` comando para acionar a exclusão automática de cópias Snapshot quando a reserva Snapshot for excedida. Por padrão, as cópias Snapshot mais antigas são excluídas primeiro.

Sobre esta tarefa

Os clones de arquivos e LUN são excluídos quando não houver mais cópias Snapshot a serem excluídas.

Passo

1. Cópias Snapshot Autodelete

   `volume snapshot autodelete modify -vserver` *`SVM`* `-volume` *`volume`* `-enabled true|false -trigger volume|snap_reserve`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir exclui automaticamente as cópias Snapshot para `vol1` quando a reserva de cópias snapshot estiver esgotada:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Restaure arquivos de cópias Snapshot

Restaurar um arquivo a partir de uma cópia Snapshot em um cliente NFS ou SMB

Um usuário em um cliente NFS ou SMB pode restaurar um arquivo diretamente de uma cópia Snapshot sem a intervenção de um administrador do sistema de storage.

Cada diretório no sistema de arquivos contém um subdiretório chamado `.snapshot` acessível para usuários NFS e SMB. O `.snapshot` subdiretório contém subdiretórios correspondentes às cópias Snapshot do volume:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Cada subdiretório contém os arquivos referenciados pela cópia Snapshot. Se os usuários excluírem ou sobrescreverem acidentalmente um arquivo, eles poderão restaurar o arquivo para o diretório de leitura e gravação pai copiando o arquivo do subdiretório Snapshot para o diretório de leitura e gravação:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Ative e desative o acesso de clientes NFS e SMB ao diretório de cópia Snapshot

Você pode ativar e desativar o acesso ao diretório cópia Snapshot usando a opção `volume modify` CLI do comando ONTAP `-snapdir-access` e, começando com ONTAP 9.10,1, você pode usar o Gerenciador do sistema para habilitar ou desabilitar sistemas cliente para acessar um diretório cópia Snapshot em um volume. A ativação do acesso torna o diretório de cópia Snapshot visível para os clientes e permite que os clientes Windows mapeem uma unidade para o diretório de cópia Snapshot para

visualizar e acessar seu conteúdo. Os clientes NFS e SMB podem restaurar um arquivo ou LUN a partir de um snapshot.

Você pode ativar ou desativar o acesso ao diretório de cópia Snapshot de um volume editando as configurações de volume ou editando as configurações de compartilhamento do volume.

Ative ou desative o acesso do cliente ao diretório de cópia Snapshot editando um volume

Passos

Você pode ativar e desativar o acesso ao diretório de cópia Snapshot do cliente usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. Por padrão, o diretório cópia Snapshot em um volume está acessível aos clientes.

System Manager

1. Clique em **armazenamento > volumes**.
2. Selecione o volume que contém o diretório cópias Snapshot que deseja exibir ou ocultar.
3. Clique ⋮ e selecione **Editar**.
4. Na seção **Configurações de cópias instantâneas (locais)**, marque ou desmarque **Mostrar o diretório cópias instantâneas para clientes**.
5. Clique em **Salvar**.

CLI

1. Verifique o status de acesso ao diretório Snapshot:

   ```
   volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
   access
   ```

   Exemplo:

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
   access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

2. Ative ou desative o acesso ao diretório cópia Instantânea:

   ```
   volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
   <true|false>
   ```

   O exemplo a seguir habilita o acesso ao diretório de cópia Snapshot no vol1:

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
   true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

Ative ou desative o acesso do cliente ao diretório de cópia Snapshot editando um compartilhamento

Por padrão, o diretório cópia Snapshot em um volume está acessível aos clientes.

Passos

1. Clique em **armazenamento > compartilhamentos**.
2. Selecione o volume que contém o diretório cópias Snapshot que deseja exibir ou ocultar.

3. Clique ⋮ e selecione **Editar**.
4. Na seção **Propriedades de compartilhamento**, marque ou desmarque **permitir que os clientes acessem o diretório cópias Snapshot**.
5. Clique em **Salvar**.

Restaurar um único arquivo a partir de uma cópia Snapshot

Você pode usar o `volume snapshot restore-file` comando para restaurar um único arquivo ou LUN a partir de uma cópia Snapshot. Você pode restaurar o arquivo para um local diferente no volume de leitura e gravação pai se não quiser substituir um arquivo existente.

Sobre esta tarefa

Se você estiver restaurando um LUN existente, um clone de LUN será criado e feito backup na forma de uma cópia Snapshot. Durante a operação de restauração, você pode ler e gravar no LUN.

Os arquivos com fluxos são restaurados por padrão.

Passos

1. Listar as cópias Snapshot em um volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as cópias Snapshot `vol1` no :

   ```
   clus1::> volume snapshot show -vserver vs1 -volume vol1

   Vserver Volume Snapshot                State    Size  Total% Used%
   ------- ------ ---------- ----------- ------   -----  ------ -----
   vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
                  daily.2013-01-25_0010   valid   92KB      0%    0%
                  hourly.2013-01-25_0105  valid   228KB     0%    0%
                  hourly.2013-01-25_0205  valid   236KB     0%    0%
                  hourly.2013-01-25_0305  valid   244KB     0%    0%
                  hourly.2013-01-25_0405  valid   244KB     0%    0%
                  hourly.2013-01-25_0505  valid   244KB     0%    0%

   7 entries were displayed.
   ```

2. Restaurar um arquivo a partir de uma cópia Snapshot:

   `volume snapshot restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-restore-path` *`destination_path`*

   Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir restaura o arquivo `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Restaure parte de um arquivo a partir de uma cópia Snapshot

Você pode usar o `volume snapshot partial-restore-file` comando para restaurar um intervalo de dados de uma cópia Snapshot para um LUN ou para um arquivo de contentor NFS ou SMB, supondo que você saiba o deslocamento de byte inicial dos dados e a contagem de bytes. Você pode usar esse comando para restaurar um dos bancos de dados em um host que armazena vários bancos de dados no mesmo LUN.

A partir do ONTAP 9.12,1, a restauração parcial está disponível para volumes usando Sincronização ativa do SnapMirroro .

Passos

1. Listar as cópias Snapshot em um volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as cópias Snapshot `vol1` no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure parte de um arquivo a partir de uma cópia Snapshot:

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   O desvio de byte inicial e a contagem de bytes devem ser múltiplos de 4.096.

O exemplo a seguir restaura os primeiros 4.096 bytes do arquivo `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Restaure o conteúdo de um volume a partir de uma cópia Snapshot

Você pode recuperar um volume para um ponto anterior no tempo restaurando a partir de uma cópia Snapshot. Você pode usar o System Manager ou o `volume snapshot restore` comando para restaurar o conteúdo de um volume a partir de uma cópia Snapshot.

Sobre esta tarefa

Se o volume tiver relações SnapMirror, replique manualmente todas as cópias espelhadas do volume imediatamente após a restauração a partir de uma cópia Snapshot. Não fazer isso pode resultar em cópias espelhadas inutilizáveis que devem ser excluídas e recriadas.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para restaurar a partir de uma cópia Snapshot anterior.

System Manager

1. Clique em **armazenamento** e selecione um volume.
2. Em **cópias Snapshot**, clique ⋮ ao lado da cópia Snapshot que deseja restaurar e selecione **Restaurar**.

CLI

1. Listar as cópias Snapshot em um volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra as cópias Snapshot `vol1` no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure o conteúdo de um volume a partir de uma cópia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

O exemplo a seguir restaura o conteúdo `vol1` de :

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Replicação de volume SnapMirror

Noções básicas de recuperação de desastres assíncrona do SnapMirror

SnapMirror é uma tecnologia de recuperação de desastres, projetada para failover de armazenamento primário para armazenamento secundário em um local geograficamente remoto. Como o nome indica, o SnapMirror cria uma réplica, ou *mirror,* dos seus dados de trabalho em armazenamento secundário a partir do qual você pode continuar a servir dados em caso de uma catástrofe no local principal.

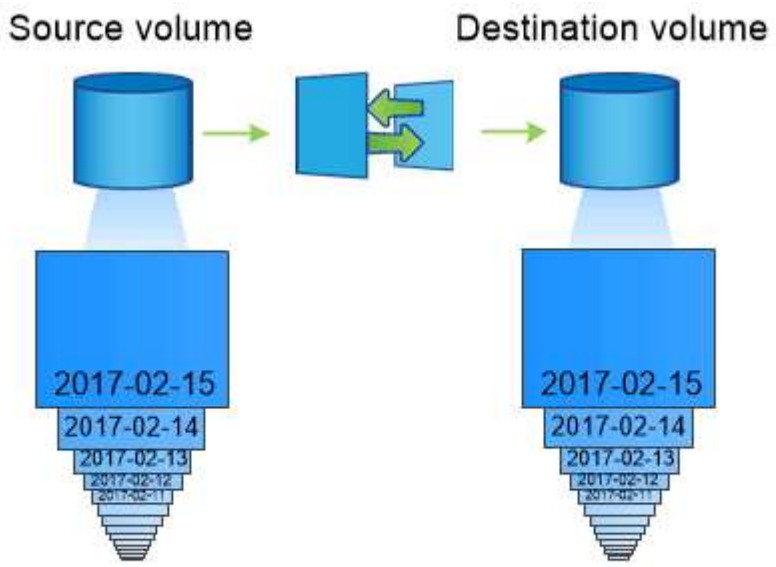
Se o site principal ainda estiver disponível para fornecer dados, você pode simplesmente transferir quaisquer dados necessários de volta para ele e não atender clientes do espelho. Como o caso de uso de failover indica, as controladoras no sistema secundário devem ser equivalentes ou quase equivalentes às controladoras no sistema primário para atender dados com eficiência do storage espelhado.

Relações de proteção de dados

Os dados são espelhados no nível do volume. A relação entre o volume de origem no armazenamento primário e o volume de destino no armazenamento secundário é chamada de *relação de proteção de dados.* os clusters nos quais os volumes residem e os SVMs que servem dados dos volumes devem ser *peered.* Uma relação de mesmo nível permite que clusters e SVMs troquem dados com segurança.

"Peering de cluster e SVM"

A figura abaixo ilustra as relações de proteção de dados da SnapMirror.



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

Escopo das relações de proteção de dados

Você pode criar uma relação de proteção de dados diretamente entre volumes ou entre as SVMs que possuem os volumes. Em uma relação de proteção de dados *SVM,* toda ou parte da configuração SVM, de exportações de NFS e compartilhamentos de SMB para RBAC, são replicados, bem como os dados nos volumes proprietários do SVM.

Você também pode usar o SnapMirror para aplicativos especiais de proteção de dados:

- Uma cópia do volume raiz do SVM garante que os dados permaneçam acessíveis em caso de interrupção ou failover de nó.
- Uma relação de proteção de dados entre o *SnapLock volumes* permite replicar arquivos WORM para um storage secundário.

  "Arquivamento e conformidade com a tecnologia SnapLock"

- A partir do ONTAP 9.13,1, você pode usar o SnapMirror assíncrono para proteger grupos de consistência. A partir do ONTAP 9.14,1, você pode usar o SnapMirror assíncrono para replicar snapshots granular de volume para o cluster de destino usando a relação de grupo de consistência. Para obter mais informações, Configurar a proteção assíncrona do SnapMirrorconsulte .

Como as relações de proteção de dados do SnapMirror são inicializadas

Na primeira vez que você invocar o SnapMirror, ele executa uma *transferência de linha de base* do volume de origem para o volume de destino. A política *SnapMirror* da relação define o conteúdo da linha de base e quaisquer atualizações.

Uma transferência de linha de base sob a política SnapMirror padrão `MirrorAllSnapshots` envolve as seguintes etapas:

- Faça uma cópia Snapshot do volume de origem.
- Transfira a cópia Snapshot e todos os blocos de dados que ela faz referência ao volume de destino.
- Transfira as cópias Snapshot restantes e menos recentes no volume de origem para o volume de destino para o caso de o espelhamento "ativo" estar corrompido.

Como os relacionamentos de proteção de dados da SnapMirror são atualizados

As atualizações são assíncronas, seguindo a programação configurada. A retenção espelha a política do Snapshot na origem.

Em cada atualização sob `MirrorAllSnapshots` a política, o SnapMirror cria uma cópia Snapshot do volume de origem e transfere essa cópia Snapshot e todas as cópias Snapshot feitas desde a última atualização. Na saída a seguir do `snapmirror policy show` comando para a `MirrorAllSnapshots` política, observe o seguinte:

- `Create Snapshot` É "verdadeiro", indicando que `MirrorAllSnapshots` cria uma cópia Snapshot quando o SnapMirror atualiza o relacionamento.
- `MirrorAllSnapshots` Tem regras "sm_created" e "all_source_snapshots", indicando que tanto a cópia Snapshot criada pelo SnapMirror quanto todas as cópias snapshot que foram feitas desde a última atualização são transferidas quando o SnapMirror atualiza a relação.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

Política MirrorLatest

A política pré-configurada `MirrorLatest` funciona exatamente da mesma forma que `MirrorAllSnapshots`, exceto que apenas a cópia Snapshot criada pelo SnapMirror é transferida na inicialização e atualização.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

Noções básicas de recuperação de desastres síncrona SnapMirror

A partir do ONTAP 9.5, a tecnologia SnapMirror Synchronous (SM-S) é suportada em todas as plataformas FAS e AFF que tenham pelo menos 16 GB de memória e em todas as plataformas ONTAP Select. A tecnologia síncrona SnapMirror é um recurso licenciado

por nó que fornece replicação de dados síncrona no nível do volume.

Esse recurso atende aos mandatos regulatórios e nacionais para replicação síncrona nos setores financeiro, de saúde e outros que tenham regulamentação com perda de dados zero.

Operações síncronas do SnapMirror permitidas

O limite do número de operações de replicação síncrona SnapMirror por par de HA depende do modelo de controladora.

A tabela a seguir lista o número de operações síncronas do SnapMirror permitidas por par de HA de acordo com o tipo de plataforma e o lançamento do ONTAP.

Plataforma	Versões anteriores ao ONTAP 9.9,1	ONTAP 9.9,1	ONTAP 9.10,1	ONTAP 9.11,1 através de ONTAP 9.14,1
AFF	80	160	200	400
ASA	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

Recursos suportados

A tabela a seguir indica os recursos compatíveis com o SnapMirror Synchronous e as versões do ONTAP nas quais o suporte está disponível.

Recurso	Lançamento primeiro suportado	Informações adicionais
Antivírus sobre o volume principal da relação síncrona SnapMirror	ONTAP 9,6	
Replicação de cópia Snapshot criada pela aplicação	ONTAP 9,7	Se uma cópia Snapshot estiver marcada com o rótulo apropriado no momento `snapshot create` da operação, usando a CLI ou a API ONTAP, o SnapMirror Synchronous replica as cópias Snapshot, criadas pelo usuário ou criadas com scripts externos, após a desativação das aplicações. As cópias Snapshot programadas criadas usando uma política Snapshot não são replicadas. Para obter mais informações sobre como replicar cópias Snapshot criadas por aplicativos, consulte o artigo da base de dados de Conhecimento: "Como replicar snapshots criados pela aplicação com o SnapMirror síncrono".
Clonar a eliminação automática	ONTAP 9,6	

Agregados FabricPool com política de disposição em camadas nenhuma, Snapshot ou Automático são compatíveis com origem e destino síncronos SnapMirror.	ONTAP 9,5	O volume de destino em um agregado do FabricPool não pode ser definido para todas as políticas de disposição em camadas.
FC	ONTAP 9,5	Em todas as redes para as quais a latência não exceda 10ms ms
FC-NVMe	ONTAP 9,7	
Clones de arquivos	ONTAP 9,7	
FPolicy no volume principal da relação síncrona SnapMirror	ONTAP 9,6	
Cotas rígidas e flexíveis sobre o volume primário do relacionamento síncrono SnapMirror	ONTAP 9,6	As regras de cota não são replicadas para o destino; portanto, o banco de dados de cota não é replicado para o destino.
Relações síncronas intra-cluster	ONTAP 9.14,1	Alta disponibilidade é fornecida quando os volumes de origem e destino são colocados em diferentes pares de HA. Se todo o cluster ficar inativo, o acesso aos volumes não será possível até que o cluster seja recuperado. As relações síncronas de SnapMirror intramcluster contribuirão para o limite geral de simultâneos Relacionamentos por par de HA.
ISCSI	ONTAP 9,5	
Clones de LUN e clones de namespace NVMe	ONTAP 9,7	
Clones de LUN com respaldo de cópias Snapshot criadas pela aplicação	ONTAP 9,7	
Acesso a protocolo misto (NFS v3 e SMB)	ONTAP 9,6	
Restauração NDMP/NDMP	ONTAP 9.13,1	Tanto o cluster de origem quanto o de destino devem estar executando o ONTAP 9.13,1 ou posterior para usar o NDMP com o SnapMirror Synchronous. Para obter mais informações, Transfira dados usando cópia ndmpconsulte .
Operações síncronas de SnapMirror (NDO) sem interrupções em plataformas AFF/ASA, somente.	ONTAP 9.12,1	O suporte a operações sem interrupções permite que você execute muitas tarefas de manutenção comuns sem agendar o tempo de inatividade. As operações suportadas incluem takeover e giveback e movimentação de volume, desde que um único nó sobreviva a cada um dos dois clusters.
NFS v4.2	ONTAP 9.10,1	
NFS v4.3	ONTAP 9,5	
NFS v4.0	ONTAP 9,6	
NFS v4.1	ONTAP 9,6	

NVMe/TCP	9.10.1	
Remoção de limitação de frequência de operação de metadados elevados	ONTAP 9,6	
Segurança para dados confidenciais em trânsito usando criptografia TLS 1,2	ONTAP 9,6	
Restauração de arquivo único e parcial	ONTAP 9.13,1	
SMB 2,0 ou posterior	ONTAP 9,6	
Cascata de espelho-espelho síncrono SnapMirror	ONTAP 9,6	A relação do volume de destino da relação síncrona do SnapMirror deve ser uma relação assíncrona do SnapMirror.
Recuperação de desastres da SVM	ONTAP 9,6	* Uma fonte síncrona SnapMirror também pode ser uma fonte de recuperação de desastres do SVM, por exemplo, uma configuração de fan-out com SnapMirror síncrono como uma etapa e a recuperação de desastres do SVM, como a outra. * Uma fonte síncrona SnapMirror não pode ser um destino de recuperação de desastres da SVM, pois o SnapMirror síncrono não oferece suporte a uma fonte de proteção de dados em cascata. É necessário liberar a relação síncrona antes de executar uma flip-ressincronização da recuperação de desastres da SVM no cluster de destino. * Um destino síncrono do SnapMirror não pode ser uma fonte de recuperação de desastres do SVM, pois a recuperação de desastres do SVM não dá suporte à replicação de volumes de DP. Uma nova sincronização da fonte síncrona resultaria na recuperação de desastres da SVM, excluindo o volume de DP no cluster de destino.
Restauração baseada em fita para o volume de origem	ONTAP 9.13,1	
Paridade de carimbo de data/hora entre volumes de origem e destino para nas	ONTAP 9,6	Se você atualizou do ONTAP 9.5 para o ONTAP 9.6, o carimbo de data/hora será replicado apenas para quaisquer arquivos novos e modificados no volume de origem. O carimbo de data/hora dos arquivos existentes no volume de origem não é sincronizado.

Funcionalidades não suportadas

Os recursos a seguir não são compatíveis com relacionamentos síncronos do SnapMirror:

- Grupos de consistência
- Sistemas DP_Optimized (DPO)
- Volumes FlexGroup
- Volumes FlexCache
- Limitação global

- Em uma configuração de fan-out, apenas uma relação pode ser uma relação síncrona do SnapMirror; todas as outras relações do volume de origem devem ser relações assíncronas do SnapMirror.
- Movimento LUN
- Configurações do MetroCluster
- LUNs de acesso mistos SAN e NVMe e namespaces NVMe não são compatíveis com o mesmo volume ou SVM.
- SnapCenter
- Volumes SnapLock
- Cópias Snapshot à prova de violações
- Backup ou restauração em fita usando dump e SMTape no volume de destino
- Piso de taxa de transferência (QoS min) para volumes de origem
- Volume SnapRestore
- VVol

Modos de funcionamento

O SnapMirror Synchronous tem dois modos de operação com base no tipo da política SnapMirror usada:

- **Modo de sincronização** no modo de sincronização, as operações de e/S do aplicativo são enviadas em paralelo aos sistemas de armazenamento primário e secundário. Se a gravação no storage secundário não for concluída por qualquer motivo, o aplicativo poderá continuar gravando no storage primário. Quando a condição de erro é corrigida, a tecnologia síncrona SnapMirror ressincroniza automaticamente com o storage secundário e retoma a replicação do storage primário para o storage secundário no modo síncrono. No modo de sincronização, o RPO 0 e o rto são muito baixos até que ocorra uma falha de replicação secundária no momento em que o RPO e o rto se tornam indeterminados, mas equivalem ao tempo de reparar o problema que fez com que a replicação secundária falhasse e para que o ressync fosse concluído.
- **Modo StrictSync** SnapMirror síncrono pode operar opcionalmente no modo StrictSync. Se a gravação no storage secundário não for concluída por qualquer motivo, a e/S do aplicativo falhará, garantindo assim que o storage primário e secundário sejam idênticos. A e/S da aplicação para o primário é retomada somente após a relação SnapMirror retornar ao `InSync` status. Se o storage primário falhar, a e/S da aplicação poderá ser retomada no storage secundário, após o failover, sem perda de dados. No modo StrictSync, o RPO é sempre zero, e o rto é muito baixo.

Status do relacionamento

O status de uma relação síncrona SnapMirror está sempre no `InSync` status durante a operação normal. Se a transferência SnapMirror falhar por qualquer motivo, o destino não está sincronizado com a origem e pode ir para o `OutofSync` status.

Para relações síncronas do SnapMirror, o sistema verifica automaticamente o status da relação `InSync`ou `OutofSync`) em um intervalo fixo. Se o status do relacionamento for `OutofSync`, o ONTAP acionará automaticamente o processo de ressincronização automática para trazer de volta a relação ao `InSync` status. A ressincronização automática é acionada apenas se a transferência falhar devido a qualquer operação, como failover não planejado de armazenamento na origem ou destino ou uma interrupção de rede. Operações iniciadas pelo usuário, `snapmirror quiesce` como e `snapmirror break` não acionam a ressincronização automática.

Se o status do relacionamento se tornar `OutofSync` para um relacionamento síncrono SnapMirror no modo

StrictSync, todas as operações de e/S para o volume primário serão interrompidas. `OutofSync`O estado da relação síncrona SnapMirror no modo de sincronização não causa interrupções para as operações primárias e/S são permitidas no volume primário.

Informações relacionadas

"Relatório técnico da NetApp 4733: Configuração síncrona da SnapMirror e práticas recomendadas"

Políticas de proteção padrão

O ONTAP inclui várias políticas de proteção padrão que você pode usar para seus relacionamentos de proteção de dados. A política que você usa depende do tipo de relação de proteção.

Se as políticas padrão não atenderem às suas necessidades de relacionamentos de proteção de dados, você poderá "crie uma política personalizada".

Lista de políticas e descrições de proteção padrão

As políticas de proteção padrão e seus tipos de política associados são descritos abaixo.

Nome	Descrição	Tipo de política
Assíncrono	Uma política unificada de cofre e assíncrono SnapMirror para espelhamento do sistema de arquivos ativo mais recente e snapshots diários e semanais com um agendamento de transferência por hora.	Assíncrono
AutomatedFailOver	Política para SnapMirror síncrona com garantia de rto zero, em que a e/S do cliente não será interrompida em caso de falha de replicação.	Síncrono
AutomatedFailOverDuplex	Política para SnapMirror síncrono com garantia de rto zero e replicação de sincronização bidirecional.	Síncrono
CloudBackupDefault	Política de cofre com regra diária.	Assíncrono
Contínuo	Política para espelhamento de bucket S3.	Contínuo
DailyBackup	Política de cofre com uma regra diária e um cronograma de transferência diário.	Assíncrono
DPDefault	Política assíncrona do SnapMirror para espelhamento de todas as cópias Snapshot e do sistema de arquivos ativo mais recente.	Assíncrono
MirrorAllinstantâneos	Política assíncrona do SnapMirror para espelhamento de todos os snapshots e o sistema de arquivos ativo mais recente.	Assíncrono
MirrorAllSnapshotsDiscardNetwork	Política assíncrona do SnapMirror para espelhamento de todos os snapshots e o sistema de arquivos ativo mais recente, excluindo as configurações de rede.	Assíncrono

Nome	Descrição	Tipo de política
MirrorAndVault	Uma política unificada de cofre e assíncrono do SnapMirror para espelhamento do sistema de arquivos ativo mais recente e snapshots diários e semanais.	Assíncrono
MirrorAndVaultDiscardNetwork	Uma política unificada de cofre e assíncrono SnapMirror para espelhamento do sistema de arquivos ativo mais recente e instantâneos diários e semanais, excluindo as configurações de rede.	Assíncrono
MirrorLatest	Política assíncrona do SnapMirror para espelhamento do sistema de arquivos ativo mais recente.	Assíncrono
SnapCenterSync	Política para SnapMirror síncrono para SnapCenter com a configuração Snapshot criada pela aplicação.	Síncrono
StrictSync	Política para SnapMirror síncrono em que o acesso do cliente será interrompido em caso de falha de replicação.	Síncrono
Síncrono	Política para SnapMirror síncrono em que o acesso do cliente não será interrompido em caso de falha de replicação.	Síncrono
Unified7year	Política de SnapMirror unificado com retenção de 7 anos.	Assíncrono
XDPDefat	Política de cofre com regras diárias e semanais.	Assíncrono

Sobre workloads compatíveis com políticas de StrictSync e sincronização

As políticas StrictSync e Sync são compatíveis com todas as aplicações baseadas em LUN com protocolos FC, iSCSI e FC-NVMe, bem como com os protocolos NFSv3 e NFSv4 para aplicações empresariais, como bancos de dados, VMware, cota, SMB etc. A partir do ONTAP 9.6, o SnapMirror síncrono pode ser usado para serviços de arquivos empresariais, como automação de design eletrônico (EDA), diretórios base e workloads de compilação de software.

No ONTAP 9.5, para uma política de sincronização, você precisa considerar alguns aspectos importantes ao selecionar as cargas de trabalho NFSv3 ou NFSv4. A quantidade de operações de leitura ou gravação de dados por workloads não é uma consideração, já que a política de sincronização pode lidar com workloads de e/S de alta leitura ou gravação. No ONTAP 9.5, as cargas de trabalho que têm criação excessiva de arquivos, criação de diretórios, alterações de permissão de arquivo ou alterações de permissão de diretório podem não ser adequadas (essas são chamadas de cargas de trabalho de alto metadados). Um exemplo típico de um workload de metadados altos é um workload de DevOps no qual você cria vários arquivos de teste, executa a automação e exclui os arquivos. Outro exemplo é a carga de trabalho de compilação paralela que gera vários arquivos temporários durante a compilação. O impactos de uma alta taxa de atividade de metadados de gravação é que ela pode fazer com que a sincronização entre espelhos quebre temporariamente, o que bloqueia o iOS de leitura e gravação do cliente.

A partir do ONTAP 9.6, essas limitações são removidas e o SnapMirror síncrono pode ser usado para workloads de serviços de arquivos empresariais que incluem ambientes de vários usuários, como diretórios base e workloads de compilação de software.

Informações relacionadas

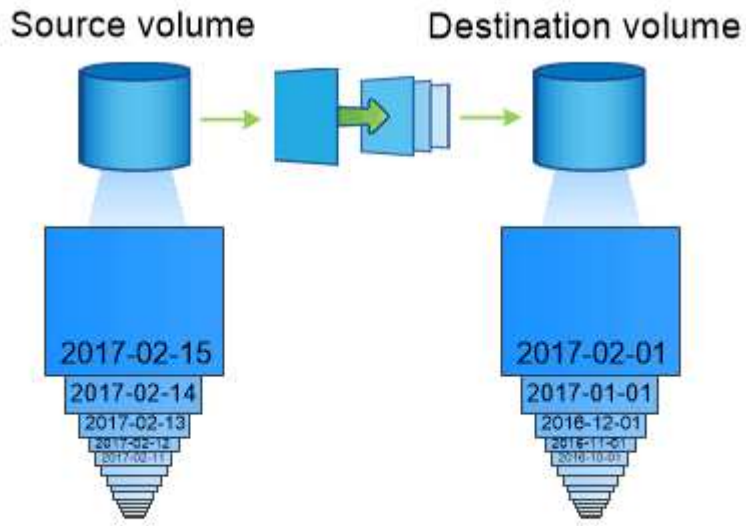
"Configuração síncrona SnapMirror e práticas recomendadas"

Arquivamento de cofre usando a tecnologia SnapMirror

As políticas do SnapMirror Vault substituem a tecnologia SnapVault no ONTAP 9.3 e posterior. Você usa uma política de cofre do SnapMirror para replicação de cópia Snapshot de disco para disco para conformidade com padrões e outros fins relacionados à governança. Em contraste com uma relação do SnapMirror, em que o destino geralmente contém apenas as cópias Snapshot atualmente no volume de origem, um destino do Vault normalmente retém cópias Snapshot pontuais criadas por um período muito mais longo.

Por exemplo, você pode manter cópias Snapshot mensais de seus dados em um período de 20 anos, para cumprir com as regulamentações contábeis governamentais dos seus negócios. Como não há necessidade de fornecer dados do armazenamento do Vault, você pode usar discos mais lentos e menos caros no sistema de destino.

A figura abaixo ilustra as relações de proteção de dados do SnapMirror Vault.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Como as relações de proteção de dados do Vault são inicializadas

A política SnapMirror para o relacionamento define o conteúdo da linha de base e quaisquer atualizações.

Uma transferência de linha de base sob a política de Vault padrão `XDPDefault` faz uma cópia Snapshot do volume de origem e, em seguida, transfere essa cópia e os dados bloqueiam as referências ao volume de destino. Diferentemente dos relacionamentos do SnapMirror, um backup de Vault não inclui cópias Snapshot mais antigas na linha de base.

Como os relacionamentos de proteção de dados do Vault são atualizados

As atualizações são assíncronas, seguindo a programação configurada. As regras definidas na política de relacionamento identificam quais novas cópias snapshot devem incluir nas atualizações e quantas cópias devem ser mantidas. Os rótulos definidos na política ("em quarto lugar", por exemplo) devem corresponder a um ou mais rótulos definidos na política de captura instantânea na origem. Caso contrário, a replicação falha.

Em cada atualização sob `XDPDefault` a política, o SnapMirror transfere cópias Snapshot feitas desde a última atualização, desde que tenham rótulos que correspondam aos rótulos definidos nas regras da política. Na saída a seguir do `snapmirror policy show` comando para a `XDPDefault` política, observe o seguinte:

- `Create Snapshot` É falso, indicando que `XDPDefault` não cria uma cópia Snapshot quando o SnapMirror atualiza a relação.
- `XDPDefault` Tem regras "diárias" e "semanais", indicando que todas as cópias Snapshot com rótulos correspondentes na origem são transferidas quando o SnapMirror atualiza o relacionamento.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                    Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Noções básicas de replicação unificada da SnapMirror

O SnapMirror *Unified replication* permite configurar a recuperação de desastres e o arquivamento no mesmo volume de destino. Quando a replicação unificada é apropriada,

ela oferece benefícios na redução da quantidade de storage secundário de que você precisa, limitando o número de transferências de linha de base e diminuindo o tráfego de rede.

Como os relacionamentos de proteção de dados unificada são inicializados

Assim como no SnapMirror, a proteção de dados unificada realiza uma transferência de linha de base na primeira vez que você a invoca. A política SnapMirror para o relacionamento define o conteúdo da linha de base e quaisquer atualizações.

Uma transferência de linha de base sob a política de proteção de dados unificada padrão `MirrorAndVault` faz uma cópia Snapshot do volume de origem e, em seguida, transfere essa cópia e os blocos de dados que ela faz referência ao volume de destino. Assim como o arquivamento de cofres, a proteção de dados unificada não inclui cópias Snapshot mais antigas na linha de base.

Como os relacionamentos unificados de proteção de dados são atualizados

Em cada atualização sob `MirrorAndVault` a política, o SnapMirror cria uma cópia Snapshot do volume de origem e transfere essa cópia Snapshot e todas as cópias Snapshot feitas desde a última atualização, desde que tenham rótulos que correspondam aos rótulos definidos nas regras de política de snapshot. Na saída a seguir do `snapmirror policy show` comando para a `MirrorAndVault` política, observe o seguinte:

- `Create Snapshot` É "verdadeiro", indicando que `MirrorAndVault` cria uma cópia Snapshot quando o SnapMirror atualiza o relacionamento.
- `MirrorAndVault` Tem regras "sm_created", "daily" e "semanal", indicando que tanto a cópia Snapshot criada pelo SnapMirror quanto as cópias Snapshot com rótulos correspondentes na fonte são transferidas quando o SnapMirror atualiza a relação.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Política do Unified7year

A política pré-configurada `Unified7year` funciona exatamente da mesma maneira que `MirrorAndVault`o , exceto que uma quarta regra transfere cópias Snapshot mensais e as retém por sete anos.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
--------- ------
                               sm_created              1  false       0 -
-
                               daily                   7  false       0 -
-
                               weekly                 52  false       0 -
-
                               monthly                84  false       0 -
-
```

Proteja-se contra possíveis corrupção de dados

A replicação unificada limita o conteúdo da transferência da linha de base para a cópia Snapshot criada pelo SnapMirror na inicialização. Em cada atualização, o SnapMirror cria outra cópia Snapshot da origem e transfere essa cópia Snapshot e quaisquer novas cópias Snapshot que tenham rótulos correspondentes aos rótulos definidos nas regras de política do Snapshot.

Você pode se proteger contra a possibilidade de que uma cópia Snapshot atualizada seja corrompida criando uma cópia da última cópia Snapshot transferida no destino. Essa cópia local é mantida independentemente das regras de retenção na origem, de modo que, mesmo que o Snapshot originalmente transferido pelo SnapMirror não esteja mais disponível na origem, uma cópia dele estará disponível no destino.

Quando usar a replicação de dados unificada

Você precisa pesar o benefício de manter um espelhamento completo em relação às vantagens que a replicação unificada oferece na redução da quantidade de storage secundário, na limitação do número de transferências de linha de base e na diminuição do tráfego de rede.

O fator chave para determinar a adequação da replicação unificada é a taxa de alteração do sistema de arquivos ativo. Um espelho tradicional pode ser mais adequado para um volume que armazena cópias Snapshot por hora de logs de transações de banco de dados, por exemplo.

O XDP substitui o DP como o padrão SnapMirror

A partir do ONTAP 9.3, o modo SnapMirror Extended Data Protection (XDP) substitui o modo SnapMirror Data Protection (DP) como padrão do SnapMirror.

Antes de atualizar para o ONTAP 9.12,1, você deve converter relações de tipo DP existentes para XDP antes de poder atualizar para o ONTAP 9.12,1 e versões posteriores. Para obter mais informações, "Converta uma relação de tipo DP existente para XDP"consulte .

Até o ONTAP 9.3, o SnapMirror invocado no modo DP e o SnapMirror invocado no modo XDP usavam diferentes mecanismos de replicação, com diferentes abordagens para dependência de versão:

- O SnapMirror invocado no modo DP usou um mecanismo de replicação *dependente da versão* no qual a versão do ONTAP era necessária para ser a mesma no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- O SnapMirror invocado no modo XDP usou um mecanismo de replicação *version-flexível* que suportava diferentes versões do ONTAP no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Com melhorias no desempenho, os benefícios significativos do SnapMirror flexível de versão superam a ligeira vantagem na taxa de transferência de replicação obtida com o modo dependente da versão. Por esse motivo, começando com ONTAP 9.3, o modo XDP foi feito o novo padrão, e todas as invocações do modo DP na linha de comando ou em scripts novos ou existentes são automaticamente convertidas para o modo XDP.

As relações existentes não são afetadas. Se uma relação já for do tipo DP, ela continuará sendo do tipo DP. A partir do ONTAP 9.5, o MirrorAndVault é a nova política padrão quando nenhum modo de proteção de dados é especificado ou quando o modo XDP é especificado como o tipo de relacionamento. A tabela abaixo mostra o comportamento que você pode esperar.

Se especificar…	O tipo é…	A política padrão (se você não especificar uma política) é…
DP	XDP	Espelhamento AllSnapshots (SnapMirror DR)
Nada	XDP	MirrorAndVault (replicação unificada)
XDP	XDP	MirrorAndVault (replicação unificada)

Como mostra a tabela, as políticas padrão atribuídas ao XDP em diferentes circunstâncias garantem que a conversão mantenha a equivalência funcional dos tipos antigos. É claro que você pode usar políticas diferentes conforme necessário, incluindo políticas para replicação unificada:

Se especificar…	E a política é…	O resultado é…
DP	MirrorAllinstantâneos	SnapMirror DR
XDPDefat	SnapVault	MirrorAndVault
Replicação unificada	XDP	MirrorAllinstantâneos
SnapMirror DR	XDPDefat	SnapVault

As únicas exceções à conversão são as seguintes:

- As relações de proteção de dados do SVM continuam como padrão no modo DP no ONTAP 9.3 e versões anteriores.

  A partir do ONTAP 9.4, as relações de proteção de dados do SVM passam por padrão no modo XDP.

- As relações de proteção de dados de compartilhamento de carga de volume raiz continuam a ser padrão para o modo DP.
- As relações de proteção de dados do SnapLock continuam a ser padrão para o modo DP no ONTAP 9.4 e anterior.

  A partir do ONTAP 9.5, as relações de proteção de dados do SnapLock são padrão para o modo XDP.

- As invocações explícitas do DP continuam a ser padrão para o modo DP se você definir a seguinte opção em todo o cluster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Essa opção será ignorada se você não invocar explicitamente o DP.

Quando um volume de destino cresce automaticamente

Durante uma transferência espelhada de proteção de dados, o volume de destino aumenta automaticamente em tamanho se o volume de origem tiver crescido, desde que haja espaço disponível no agregado que contenha o volume.

Este comportamento ocorre independentemente de qualquer definição de crescimento automático no destino. Você não pode limitar o crescimento do volume ou impedir que o ONTAP o aumente.

Por padrão, os volumes de proteção de dados são definidos para o `grow_shrink` modo automático, o que permite que o volume cresça ou diminua em resposta à quantidade de espaço usado. O dimensionamento automático máximo para volumes de proteção de dados é igual ao tamanho máximo de FlexVol e depende da plataforma. Por exemplo:

- FAS8200, volume DP padrão máximo-dimensionamento automático: 100TB

Para obter mais informações, "NetApp Hardware Universe"consulte .

Implantações de proteção de dados em cascata e fan-out

Você pode usar uma implantação *fan-out* para estender a proteção de dados a vários sistemas secundários. Você pode usar uma implantação *Cascade* para estender a proteção de dados para sistemas terciários.

As implantações em fan-out e em cascata são compatíveis com qualquer combinação de recuperação de desastres, SnapVault ou replicação unificada da SnapMirror. A partir do ONTAP 9.5, as relações síncronas do SnapMirror são compatíveis com implantações fan-out com uma ou mais relações assíncronas do SnapMirror. Apenas uma relação na configuração de fan-out pode ser uma relação síncrona SnapMirror, todas as outras relações do volume de origem devem ser relações assíncronas do SnapMirror. As relações síncronas do SnapMirror também são compatíveis com implantações em cascata (a partir de ONTAP 9.6). No entanto, a relação do volume de destino da relação síncrona do SnapMirror deve ser uma relação assíncrona do

SnapMirror. Sincronização ativa do SnapMirror (Suportado a partir do ONTAP 9.3,1) também suporta configurações de fan-out.

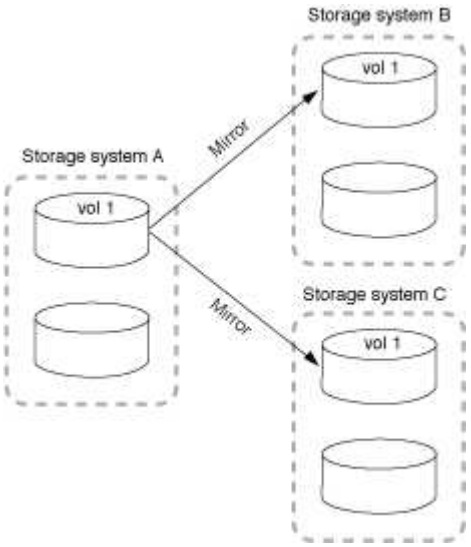
Você pode usar uma implantação *fan-in* para criar relações de proteção de dados entre vários sistemas primários e um único sistema secundário. Cada relação deve usar um volume diferente no sistema secundário.

Você deve estar ciente de que os volumes que fazem parte de uma configuração de fan-out ou cascata podem levar mais tempo para ressincronizar. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

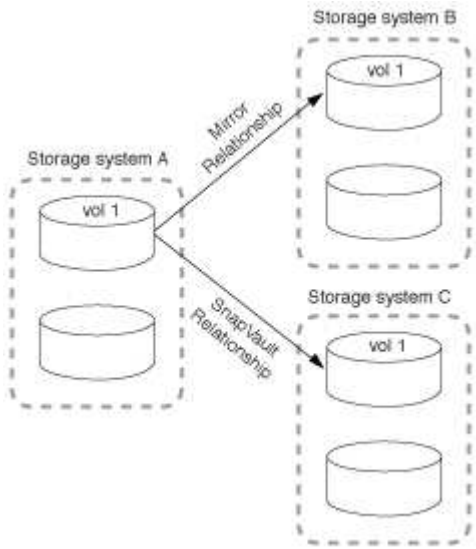
Como as implantações de fan-out funcionam

O SnapMirror suporta implantações de fan-out *multiple-mirrors* e *mirror-Vault*.

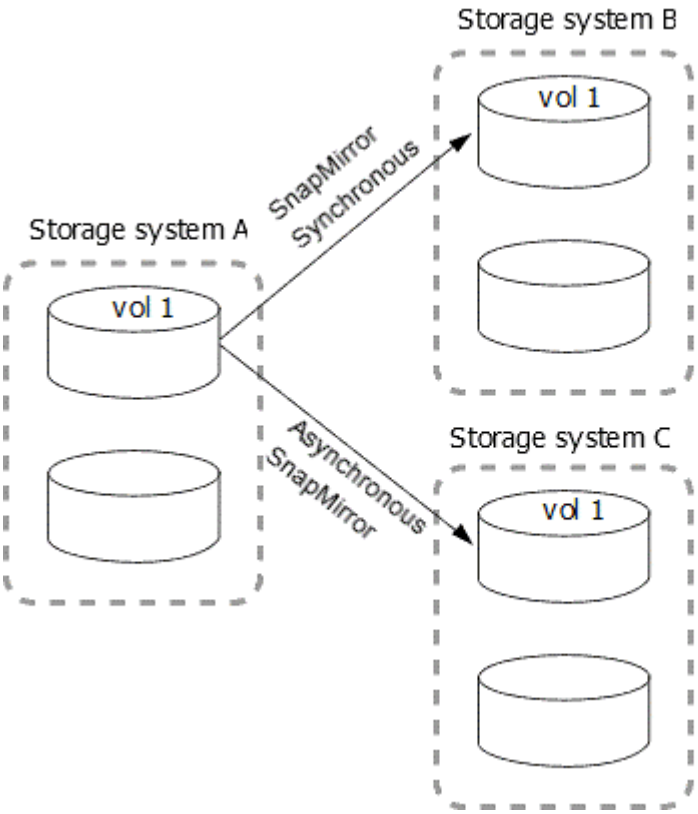
Uma implantação de fan-out de vários espelhos consiste em um volume de origem que tem uma relação espelhada com vários volumes secundários.



Uma implantação de fan-out do mirror-Vault consiste em um volume de origem que tem uma relação de espelhamento com um volume secundário e uma relação de SnapVault com um volume secundário diferente.



A partir do ONTAP 9.5, você pode ter implantações de fan-out com relacionamentos síncronos do SnapMirror; no entanto, apenas uma relação na configuração de fan-out pode ser uma relação síncrona do SnapMirror, todas as outras relações do volume de origem devem ser relações assíncronas do SnapMirror.

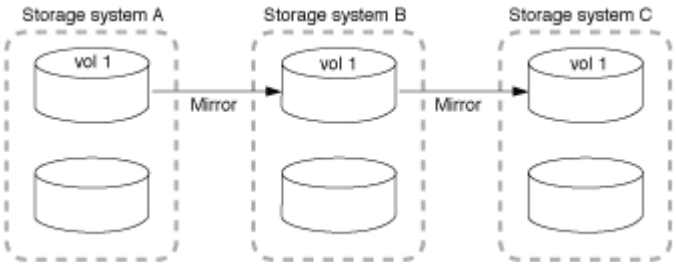


Como as implantações em cascata funcionam

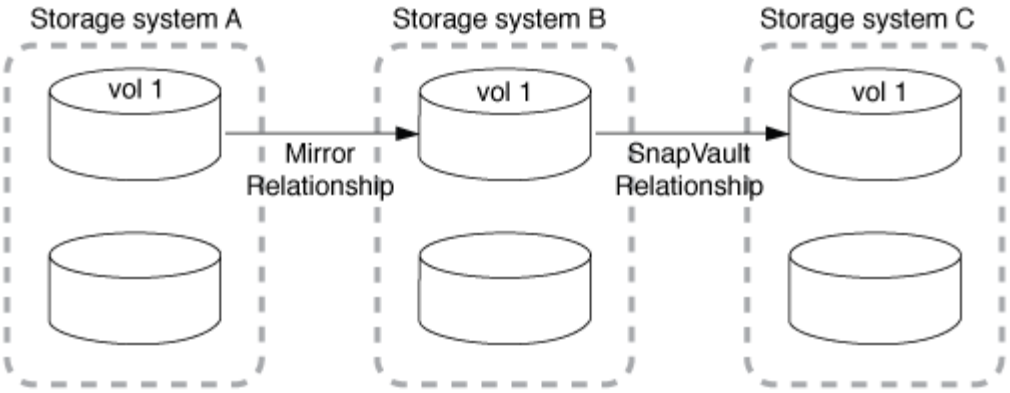
O SnapMirror suporta implantações em cascata *mirror-mirror*, *mirror-Vault*, *Vault-mirror* e *Vault-Vault*.

Uma implantação em cascata espelhada consiste em uma cadeia de relacionamentos em que um volume de origem é espelhado em um volume secundário e o volume secundário é espelhado em um volume terciário. Se o volume secundário ficar indisponível, é possível sincronizar a relação entre os volumes primário e terciário sem efetuar uma nova transferência de linha de base.

A partir do ONTAP 9.6, as relações síncronas do SnapMirror são suportadas em uma implantação em cascata espelhada. Somente os volumes primário e secundário podem estar em uma relação síncrona do SnapMirror. A relação entre os volumes secundários e os volumes terciários deve ser assíncrona.



Uma implantação em cascata de cofre-espelho consiste em uma cadeia de relacionamentos em que um volume de origem é espelhado em um volume secundário, e o volume secundário é abobadado a um volume terciário.



Vault-mirror e, a partir do ONTAP 9.2, as implantações em cascata Vault-Vault também são suportadas:

- Uma implantação em cascata de espelho de cofre consiste em uma cadeia de relacionamentos em que um volume de origem é abobadado para um volume secundário, e o volume secundário é espelhado para um volume terciário.
- (Começando com ONTAP 9.2) Uma implantação em cascata de Vault-Vault consiste em uma cadeia de relacionamentos em que um volume de origem é abobadado para um volume secundário e o volume secundário é abobadado para um volume terciário.

Leitura adicional

- Retome a proteção em uma configuração de fan-out com a sincronização ativa do SnapMirror

Licenciamento do SnapMirror

Visão geral do licenciamento do SnapMirror

A partir do ONTAP 9.3, o licenciamento foi simplificado para replicação entre instâncias do ONTAP. Nas versões do ONTAP 9, a licença do SnapMirror suporta relações de cofre e espelho. Você pode usar uma licença do SnapMirror para dar suporte à replicação do ONTAP para casos de uso de backup e recuperação de desastres.

Antes da versão do ONTAP 9.3, uma licença SnapVault separada era necessária para configurar relações *Vault* entre instâncias do ONTAP, onde a instância DP poderia reter um número maior de cópias Snapshot para suportar casos de uso de backup com tempos de retenção mais longos, e uma licença SnapMirror era necessária para configurar relações *mirror* entre instâncias do ONTAP, onde cada instância do ONTAP manteria o mesmo número de cópias Snapshot (ou seja, uma imagem *mirror*) para permitir o uso de falhas de recuperação de cluster. Ambas as licenças SnapMirror e SnapVault continuam a ser usadas e suportadas para versões do ONTAP 8.x e 9.x.

Embora as licenças do SnapVault continuem a funcionar e sejam suportadas para ambas as versões do ONTAP 8.x e 9.x, a licença do SnapMirror pode ser usada em vez de uma licença SnapVault e pode ser usada para configurações de espelhamento e cofre.

Para replicação assíncrona do ONTAP, a partir do ONTAP 9.3, um único mecanismo de replicação unificada é usado para configurar políticas de modo de proteção de dados estendida (XDP), em que a licença do SnapMirror pode ser configurada para uma política de espelhamento, uma política de cofre ou uma política de cofre-espelho. É necessária uma licença SnapMirror nos clusters de origem e destino. Uma licença SnapVault não é necessária se uma licença SnapMirror já estiver instalada. A licença perpétua assíncrona do SnapMirror está incluída no pacote de software ONTAP One que é instalado nos novos sistemas AFF e FAS.

Os limites de configuração de proteção de dados são determinados usando vários fatores, incluindo a versão do ONTAP, a plataforma de hardware e as licenças instaladas. Para obter mais informações, "Hardware Universe"consulte .

Licença síncrona SnapMirror

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas. Você precisa das seguintes licenças para criar um relacionamento síncrono do SnapMirror:

- A licença síncrona do SnapMirror é necessária no cluster de origem e no cluster de destino.

  A licença síncrona do SnapMirror faz parte do "Pacote de licenças ONTAP One".

  Se o seu sistema tiver sido adquirido antes de junho de 2019 com um pacote Premium ou Flash, você poderá baixar uma chave mestra NetApp para obter a licença síncrona SnapMirror necessária no site de suporte da NetApp: "Chaves da licença principal".

- A licença SnapMirror é necessária no cluster de origem e no cluster de destino.

Licença de nuvem da SnapMirror

A partir do ONTAP 9.8, a licença de nuvem do SnapMirror fornece replicação assíncrona de cópias Snapshot de instâncias do ONTAP para pontos de extremidade de storage de objetos. Os destinos de replicação podem ser configurados usando armazenamentos de objetos no local e serviços de storage de objetos em nuvem pública compatíveis com S3 e S3. Os relacionamentos de nuvem da SnapMirror são compatíveis com sistemas ONTAP para destinos de storage de objetos pré-qualificados.

A nuvem do SnapMirror não está disponível como uma licença autônoma. Apenas uma licença é necessária por cluster do ONTAP. Além de uma licença de nuvem do SnapMirror, a licença assíncrona do SnapMirror também é necessária.

Você precisa das seguintes licenças para criar um relacionamento de nuvem do SnapMirror:

- Uma licença SnapMirror e uma licença de nuvem SnapMirror para replicação diretamente no endpoint do armazenamento de objetos.
- Ao configurar um fluxo de trabalho de replicação de várias políticas (por exemplo, disco para disco para nuvem), é necessária uma licença SnapMirror em todas as instâncias do ONTAP, enquanto a licença de nuvem do SnapMirror é necessária apenas para o cluster de origem que está replicando diretamente para o endpoint de armazenamento de objetos.

Começando com ONTAP 9.9,1, você pode "Use o System Manager para replicação na nuvem do SnapMirror".

Uma lista de aplicativos de terceiros autorizados na nuvem da SnapMirror é publicada no site da NetApp.

Licença otimizada de proteção de dados

As licenças de proteção de dados otimizada (DPO) não estão mais sendo vendidas e o DPO não é suportado nas plataformas atuais; no entanto, se você tiver uma licença de DPO instalada em uma plataforma compatível, o NetApp continuará fornecendo suporte até o final da disponibilidade dessa plataforma.

O DPO não está incluído com o pacote de licenças ONTAP One e não pode atualizar para o pacote de licenças ONTAP One se a licença DPO estiver instalada num sistema.

Para obter informações sobre plataformas compatíveis, "Hardware Universe" consulte .

Instalar licenças de nuvem do SnapMirror

Os relacionamentos de nuvem do SnapMirror podem ser orquestrados usando aplicativos de backup de terceiros pré-qualificados. A partir do ONTAP 9.9,1, você também pode usar o System Manager para orquestrar a replicação na nuvem do SnapMirror. As licenças de capacidade de nuvem do SnapMirror e do SnapMirror são necessárias ao usar o System Manager para orquestrar ONTAP on-premises para backups de storage de objetos. Você também precisará solicitar e instalar a licença da API de nuvem do SnapMirror.

Sobre esta tarefa

A nuvem SnapMirror e as licenças do SnapMirror S3 são licenças de cluster, não de nós, portanto, elas *não* são entregues com o pacote de licenças do ONTAP One. Essas licenças estão incluídas no pacote de compatibilidade ONTAP One separado. Se você quiser habilitar a nuvem do SnapMirror, precisará solicitar este pacote.

Além disso, a orquestração do System Manager dos backups da nuvem do SnapMirror para o storage de objetos requer uma chave de API de nuvem da SnapMirror. Essa licença de API é uma licença de cluster de instância única, o que significa que não precisa ser instalada em todos os nós do cluster.

Passos

Você precisa solicitar e baixar o pacote de compatibilidade do ONTAP One e a licença da API de nuvem do SnapMirror e instalá-los usando o Gerenciador de sistema.

1. Localize e grave o UUID de cluster para o cluster que deseja licenciar.

   O UUID do cluster é necessário quando você envia sua solicitação para solicitar o pacote de compatibilidade do ONTAP One para o cluster.

2. Entre em Contato com sua equipe de vendas da NetApp e solicite o pacote de compatibilidade do ONTAP One.
3. Solicite a licença da API de nuvem da SnapMirror seguindo as instruções fornecidas no site de suporte da NetApp.

   "Solicite a chave de licença da API de nuvem da SnapMirror"

4. Quando você receber e baixar os arquivos de licença, use o Gerenciador do sistema para fazer o upload do NLF de compatibilidade da nuvem do ONTAP e do NLF da API da nuvem do SnapMirror para o cluster:
   a. Clique em **Cluster > Settings**.
   b. Na janela **Settings**, clique em **Licenses**.
   c. Na janela **Licenses**, clique + Add em .
   d. Na caixa de diálogo **Add License** (Adicionar licença), clique em **Browse** (Procurar) para selecionar o NLF transferido e, em seguida, clique em **Add** (Adicionar) para carregar o ficheiro para o cluster.

Informações relacionadas

"Faça backup dos dados na nuvem usando o SnapMirror"

"Pesquisa de licença de software NetApp"

Os sistemas DPO apresentam melhorias

A partir do ONTAP 9.6, o número máximo de volumes FlexVol suportados aumenta quando a licença DP_Optimized (DPO) é instalada. A partir do ONTAP 9.4, os sistemas com licença de DPO dão suporte a SnapMirror backoff, deduplicação em segundo plano entre volumes, uso de blocos Snapshot como doadores e compactação.

A partir do ONTAP 9.6, o número máximo de volumes FlexVol com suporte em sistemas secundários ou de proteção de dados aumentou, permitindo que você escale até 2.500 volumes FlexVol por nó ou até 5.000 TB no modo failover. O aumento dos volumes FlexVol é ativado com o "Licença DP_Optimized (DPO)". Ainda é necessário um "Licença SnapMirror"nos nós de origem e de destino.

A partir do ONTAP 9.4, os seguintes aprimoramentos de recursos são feitos nos sistemas DPO:

- SnapMirror backoff: Nos sistemas DPO, o tráfego de replicação tem a mesma prioridade que as cargas de trabalho do cliente são dadas.

  O backoff do SnapMirror é desativado por padrão nos sistemas DPO.

- Deduplicação em segundo plano do volume e deduplicação em segundo plano entre volumes: A deduplicação em segundo plano do volume e a deduplicação em segundo plano entre volumes são ativadas em sistemas DPO.

  Você pode executar `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` o comando para deduplicar os dados existentes. A prática recomendada é executar o comando durante horas fora do pico para reduzir o impactos no desempenho.

- Maior economia ao usar blocos Snapshot como doadores: Os blocos de dados que não estão disponíveis no sistema de arquivos ativo, mas estão presos em cópias Snapshot são usados como doadores para deduplicação de volume.

  Os novos dados podem ser deduplicados com os dados retidos nas cópias Snapshot. Eles também compartilham os blocos Snapshot com eficiência. O maior espaço de doadores oferece mais economia, especialmente quando o volume tem um grande número de cópias Snapshot.

- Compactação: A compactação de dados está ativada por padrão nos volumes DPO.

Gerenciar a replicação de volume do SnapMirror

Fluxo de trabalho de replicação do SnapMirror

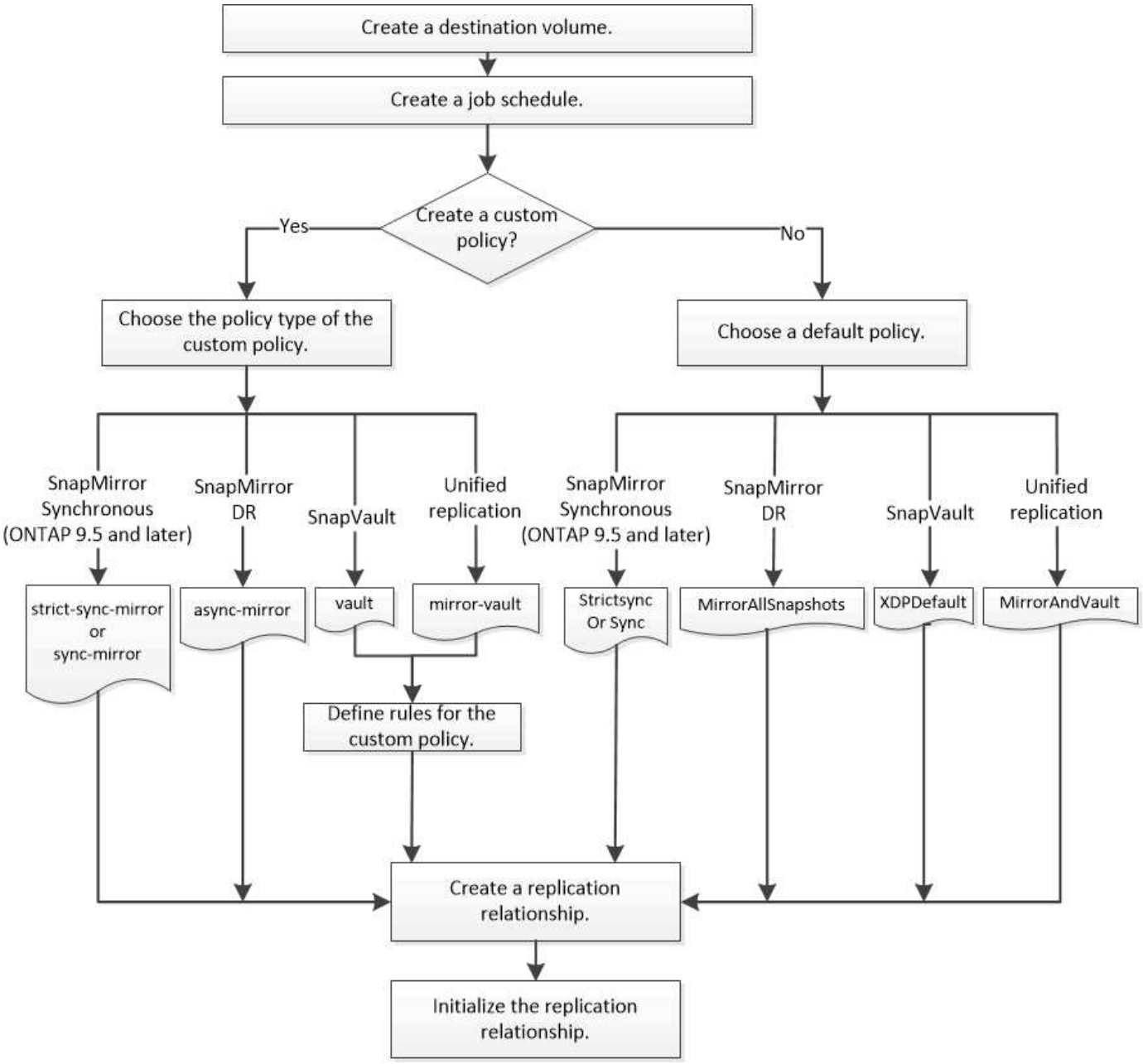
O SnapMirror oferece três tipos de relação de proteção de dados: Recuperação de desastres do SnapMirror, arquivamento (anteriormente conhecido como SnapVault) e replicação unificada. Você pode seguir o mesmo fluxo de trabalho básico para configurar cada tipo de relacionamento.

A partir da disponibilidade geral no ONTAP 9.9,1"Sincronização ativa do SnapMirror", fornece objetivo de tempo de recuperação zero (rto zero) ou failover transparente de aplicações (TAF) para permitir o failover automático de aplicações essenciais aos negócios em ambientes SAN.

Para cada tipo de relação de proteção de dados do SnapMirror, o fluxo de trabalho é o mesmo: Criar um

volume de destino, criar uma agenda de trabalho, especificar uma política, criar e inicializar a relação.

A partir do ONTAP 9.3, você pode usar o `snapmirror protect` comando para configurar uma relação de proteção de dados em uma única etapa. Mesmo que você use `snapmirror protect`o , você precisa entender cada etapa do fluxo de trabalho.



Configure uma relação de replicação em uma etapa

A partir do ONTAP 9.3, você pode usar o `snapmirror protect` comando para configurar uma relação de proteção de dados em uma única etapa. Você especifica uma lista de volumes a serem replicados, uma SVM no cluster de destino, uma programação de tarefa e uma política do SnapMirror. `snapmirror protect` faz o resto.

O que você vai precisar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

  "Peering de cluster e SVM"

- O idioma no volume de destino deve ser o mesmo que o idioma no volume de origem.

Sobre esta tarefa

`snapmirror protect`O comando escolhe um agregado associado ao SVM especificado. Se nenhum agregado estiver associado ao SVM, ele escolherá entre todos os agregados no cluster. A escolha do agregado é baseada na quantidade de espaço livre e no número de volumes no agregado.

O `snapmirror protect` comando então executa as seguintes etapas:

- Cria um volume de destino com um tipo apropriado e uma quantidade de espaço reservado para cada volume na lista de volumes a serem replicados.
- Configura uma relação de replicação apropriada para a política especificada.
- Inicializa o relacionamento.

O nome do volume de destino é do formulário *`source_volume_name_dst`*. Em caso de conflito com um nome existente, o comando adiciona um número ao nome do volume. Você pode especificar um prefixo e/ou sufixo nas opções de comando. O sufixo substitui o sufixo fornecido pelo sistema `dst`.

No ONTAP 9.3 e versões anteriores, um volume de destino pode conter até 251 cópias Snapshot. No ONTAP 9.4 e posterior, um volume de destino pode conter até 1019 cópias snapshot.

A inicialização pode ser demorada. `snapmirror protect` não espera que a inicialização seja concluída antes de o trabalho terminar. Por esse motivo, você deve usar o `snapmirror show` comando em vez do `job show` comando para determinar quando a inicialização está concluída.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror podem ser criadas usando o `snapmirror protect` comando.

Passo

1. Crie e inicialize uma relação de replicação em uma etapa:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. A `-auto-initialize` opção padrão é "'true'".

O exemplo a seguir cria e inicializa um relacionamento de DR do SnapMirror usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

Você pode usar uma política personalizada se preferir. Para obter mais informações, "Criando uma política de replicação personalizada"consulte .

O exemplo a seguir cria e inicializa um relacionamento SnapVault usando a política padrão `XDPDefault`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

O exemplo a seguir cria e inicializa uma relação de replicação unificada usando a política padrão `MirrorAndVault`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

O exemplo a seguir cria e inicializa um relacionamento síncrono do SnapMirror usando a política padrão `Sync`:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

Para políticas de replicação unificada e SnapVault, talvez seja útil definir uma programação para criar uma cópia da última cópia Snapshot transferida no destino. Para obter mais informações, "Definir uma agenda para criar uma cópia local no destino"consulte .

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Configure uma relação de replicação uma etapa de cada vez

Crie um volume de destino

Você pode usar o `volume create` comando no destino para criar um volume de destino. O volume de destino deve ser igual ou maior em tamanho do que o volume de origem.

Passo

1. Criar um volume de destino:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria um volume de destino de 2 GB chamado `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Criar um agendamento de trabalho de replicação

O agendamento de trabalhos determina quando o SnapMirror atualiza automaticamente a relação de proteção de dados à qual o agendamento é atribuído. Você pode usar o System Manager ou o `job schedule cron create` comando para criar uma agenda de trabalho de replicação.

Sobre esta tarefa

Você atribui um agendamento de trabalho ao criar um relacionamento de proteção de dados. Se não atribuir uma agenda de trabalhos, tem de atualizar a relação manualmente.

Passos

Você pode criar uma programação de trabalho de replicação usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

1. Navegue até **proteção > Visão geral** e expanda **configurações de política local**.
2. No painel **horários**, clique em .
3. Na janela **horários**, clique em .
4. Na janela **Adicionar agendamento**, insira o nome da programação e escolha o contexto e o tipo de agendamento.
5. Clique em **Salvar**.

CLI

1. Criar uma agenda de trabalhos:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

A partir do ONTAP 9.10,1, você pode incluir o SVM para sua agenda de trabalho:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

O cronograma mínimo com suporte (RPO) para volumes FlexVol em uma relação de volume SnapMirror é de 5 minutos. O cronograma mínimo com suporte (RPO) para volumes FlexGroup em uma relação de volume SnapMirror é de 30 minutos.

O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Personalizar uma política de replicação

Crie uma política de replicação personalizada

Você pode criar uma política de replicação personalizada se a política padrão para um relacionamento não for adequada. Você pode querer compactar dados em uma transferência de rede, por exemplo, ou modificar o número de tentativas que o SnapMirror faz para transferir cópias Snapshot.

Você pode usar uma política padrão ou personalizada ao criar uma relação de replicação. Para um arquivo personalizado (anteriormente SnapVault) ou uma política de replicação unificada, você deve definir uma ou mais *regras* para determinar quais cópias snapshot serão transferidas durante a inicialização e a atualização. Também é possível definir uma programação para criar cópias Snapshot locais no destino.

O *policy type* da diretiva de replicação determina o tipo de relação que ela suporta. A tabela abaixo mostra os tipos de política disponíveis.

Tipo de política	Tipo de relação
espelho assíncrono	SnapMirror DR
cofre	SnapVault
espelho-cofre	Replicação unificada
strict-sync-mirror	SnapMirror síncrono no modo StrictSync (suportado a partir de ONTAP 9.5)
espelho de sincronização	SnapMirror síncrono no modo de sincronização (suportado a partir de ONTAP 9.5)

Quando você cria uma política de replicação personalizada, é uma boa ideia modelar a política após uma política padrão.

Passos

Você pode criar políticas de proteção de dados personalizadas com o System Manager ou a CLI do ONTAP. A partir do ONTAP 9.11,1, você pode usar o Gerenciador do sistema para criar políticas de espelhamento e cofre personalizadas e exibir e selecionar políticas herdadas. Essa capacidade também está disponível no ONTAP 9.8P12 e patches posteriores do ONTAP 9.8.

Crie políticas de proteção personalizadas no cluster de origem e destino.

System Manager

1. Clique em **proteção > Visão geral > Configurações de política local**.
2. Em **políticas de proteção**, clique em .
3. No painel **políticas de proteção**, clique em Add .
4. Introduza o novo nome da política e selecione o âmbito da política.
5. Escolha um tipo de política. Para adicionar uma política somente para Vault ou somente para espelhamento, escolha **assíncrono** e clique em **usar um tipo de política legado**.
6. Preencha os campos obrigatórios.
7. Clique em **Salvar**.
8. Repita estas etapas no outro cluster.

CLI

1. Criar uma política de replicação personalizada:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

Para obter a sintaxe completa do comando, consulte a página man.

A partir do ONTAP 9.5, você pode especificar a programação para criar uma agenda comum de cópias Snapshot para relacionamentos síncronos do SnapMirror usando o `-common-snapshot-schedule` parâmetro. Por padrão, o agendamento comum de cópia Snapshot para relacionamentos síncronos do SnapMirror é de uma hora. Você pode especificar um valor de 30 minutos a duas horas para a programação da cópia Snapshot para relacionamentos síncronos do SnapMirror.

O exemplo a seguir cria uma política de replicação personalizada para o SnapMirror DR que permite a compactação de rede para transferências de dados:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

O exemplo a seguir cria uma política de replicação personalizada para o SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

O exemplo a seguir cria uma política de replicação personalizada para replicação unificada:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

O exemplo a seguir cria uma política de replicação personalizada para o relacionamento síncrono do SnapMirror no modo StrictSync:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Depois de terminar

Para os tipos de política "'Vault'" e "mirror-Vault", você deve definir regras que determinam quais cópias snapshot serão transferidas durante a inicialização e atualização.

Use o `snapmirror policy show` comando para verificar se a política SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Defina uma regra para uma política

Para políticas personalizadas com o tipo de política "'Vault'" ou "mirror-Vault", você deve definir pelo menos uma regra que determina quais cópias snapshot serão transferidas durante a inicialização e atualização. Você também pode definir regras para políticas padrão com o tipo de política "'Vault'" ou "mirror-Vault".

Sobre esta tarefa

Todas as políticas com o tipo de política "'Vault'" ou "mirror-Vault" devem ter uma regra que especifique quais cópias snapshot devem ser replicadas. A regra "bimestral", por exemplo, indica que apenas cópias Snapshot atribuídas ao rótulo "bimestral" do SnapMirror devem ser replicadas. Você especifica o rótulo SnapMirror ao configurar a política de captura instantânea na origem.

Cada tipo de política está associado a uma ou mais regras definidas pelo sistema. Essas regras são atribuídas automaticamente a uma política quando você especifica seu tipo de política. A tabela abaixo mostra as regras definidas pelo sistema.

Regra definida pelo sistema	Usado em tipos de política	Resultado
sm_created	Espelho assíncrono, espelho-Vault, sincronização, StrictSync	Uma cópia Snapshot criada pelo SnapMirror é transferida na inicialização e atualização.
all_source_snapshots	espelho assíncrono	Novas cópias Snapshot na origem são transferidas na inicialização e atualização.

diariamente	cofre, espelho-cofre	Novas cópias Snapshot na fonte com o rótulo "diário" do SnapMirror são transferidas na inicialização e atualização.
semanalmente	cofre, espelho-cofre	Novas cópias Snapshot na origem com o rótulo "semanal" do SnapMirror são transferidas na inicialização e atualização.
mensalmente	espelho-cofre	Novas cópias Snapshot na fonte com o rótulo SnapMirror "em quarto lugar" são transferidas na inicialização e atualização.
app_consistente	Sincronizar, StrictSync	As cópias snapshot com o rótulo SnapMirror "app_consistent" na origem são replicadas de forma síncrona para o destino. Suportado a partir de ONTAP 9.7.

Exceto para o tipo de política "async-mirror", você pode especificar regras adicionais conforme necessário, para políticas padrão ou personalizadas. Por exemplo:

- Para a política padrão `MirrorAndVault`, você pode criar uma regra chamada "bimestral" para combinar cópias Snapshot na origem com o rótulo SnapMirror ""bimestral"".
- Para uma política personalizada com o tipo de política "mirror-Vault", você pode criar uma regra chamada "bi-semporal" para combinar cópias Snapshot na origem com o rótulo SnapMirror "bi-semporal".

Passo

1. Defina uma regra para uma política:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir adiciona uma regra com o rótulo SnapMirror `bi-monthly` à política padrão `MirrorAndVault`:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   O exemplo a seguir adiciona uma regra com o rótulo SnapMirror `bi-weekly` à política personalizada `my_snapvault`:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

O exemplo a seguir adiciona uma regra com o rótulo SnapMirror `app_consistent` à política personalizada `Sync`:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Em seguida, é possível replicar cópias Snapshot do cluster de origem que corresponda a este rótulo SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Defina uma agenda para criar uma cópia local no destino

Para relacionamentos de replicação unificada e SnapVault, você pode se proteger contra a possibilidade de que uma cópia Snapshot atualizada seja corrompida criando uma cópia da última cópia Snapshot transferida no destino. Essa cópia local é mantida independentemente das regras de retenção na origem, de modo que, mesmo que o Snapshot originalmente transferido pelo SnapMirror não esteja mais disponível na origem, uma cópia dele estará disponível no destino.

Sobre esta tarefa

Você especifica a programação para criar uma cópia local na `-schedule` opção `snapmirror policy add-rule` do comando.

Passo

1. Defina uma agenda para criar uma cópia local no destino:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   Para obter a sintaxe completa do comando, consulte a página man. Para obter um exemplo de como criar uma agenda de trabalhos, "Criando um agendamento de trabalho de replicação"consulte .

   O exemplo a seguir adiciona uma programação para criar uma cópia local à política padrão `MirrorAndVault`:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   O exemplo a seguir adiciona uma programação para criar uma cópia local à política personalizada

`my_unified`:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Crie uma relação de replicação

A relação entre o volume de origem no storage primário e o volume de destino no storage secundário é chamada de *relação de proteção de dados.* você pode usar o `snapmirror create` comando para criar relacionamentos de proteção de dados de replicação unificada, SnapVault ou DR do SnapMirror.

> Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para criar uma relação de replicação. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A partir do ONTAP 9.11,1, você pode usar o Gerenciador do sistema para selecionar políticas de espelhamento e cofre pré-criadas e personalizadas, exibir e selecionar políticas herdadas e substituir as programações de transferência definidas em uma política de proteção ao proteger volumes e VMs de storage. Essa capacidade também está disponível no ONTAP 9.8P12 e patches posteriores do ONTAP 9.8.

> Se você estiver usando a versão de patch do ONTAP 9.8P12 ou posterior do ONTAP 9.8 e tiver configurado o SnapMirror usando o Gerenciador de sistema, use o ONTAP 9.9.1P13 ou versões de patch do ONTAP 9.10.1P10 ou versões posteriores se você planeja atualizar para versões do ONTAP 9.9,1 ou do ONTAP 9.10,1.

Antes de começar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

  "Peering de cluster e SVM"

- O idioma no volume de destino deve ser o mesmo que o idioma no volume de origem.

Sobre esta tarefa

Até o ONTAP 9.3, o SnapMirror invocado no modo DP e o SnapMirror invocado no modo XDP usavam diferentes mecanismos de replicação, com diferentes abordagens para dependência de versão:

- O SnapMirror invocado no modo DP usou um mecanismo de replicação *dependente da versão* no qual a versão do ONTAP era necessária para ser a mesma no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- O SnapMirror invocado no modo XDP usou um mecanismo de replicação *version-flexível* que suportava diferentes versões do ONTAP no storage primário e secundário:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Com melhorias no desempenho, os benefícios significativos do SnapMirror flexível de versão superam a ligeira vantagem na taxa de transferência de replicação obtida com o modo dependente da versão. Por esse motivo, começando com ONTAP 9.3, o modo XDP foi feito o novo padrão, e todas as invocações do modo DP na linha de comando ou em scripts novos ou existentes são automaticamente convertidas para o modo XDP.

As relações existentes não são afetadas. Se uma relação já for do tipo DP, ela continuará sendo do tipo DP. A tabela abaixo mostra o comportamento que você pode esperar.

Se especificar…	O tipo é…	A política padrão (se você não especificar uma política) é…
DP	XDP	Espelhamento AllSnapshots (SnapMirror DR)
Nada	XDP	Espelhamento AllSnapshots (SnapMirror DR)
XDP	XDP	XDPDefault (SnapVault)

Veja também os exemplos no procedimento abaixo.

As únicas exceções à conversão são as seguintes:

- As relações de proteção de dados do SVM continuam como padrão no modo DP.

  Especifique XDP explicitamente para obter o modo XDP com a política padrão `MirrorAllSnapshots`.

- As relações de proteção de dados de compartilhamento de carga continuam para o modo DP padrão.
- As relações de proteção de dados do SnapLock continuam a ser padrão para o modo DP.
- As invocações explícitas do DP continuam a ser padrão para o modo DP se você definir a seguinte opção em todo o cluster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Essa opção será ignorada se você não invocar explicitamente o DP.

No ONTAP 9.3 e versões anteriores, um volume de destino pode conter até 251 cópias Snapshot. No ONTAP 9.4 e posterior, um volume de destino pode conter até 1019 cópias snapshot.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas.

A partir de ONTAP 9.14,1, a `-backoff-level` opção é adicionada aos `snapmirror create` comandos , `snapmirror modify` e `snapmirror restore` para permitir que você especifique o nível de backoff por relacionamento. A opção é suportada apenas com relacionamentos FlexVol SnapMirror. O comando opcional especifica o nível de backoff do SnapMirror devido às operações do cliente. Os valores de backoff podem ser altos, médios ou nenhum. O valor padrão é alto.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para criar uma relação de replicação.

System Manager

1. Selecione o volume ou LUN a proteger: Clique em **armazenamento > volumes** ou **armazenamento > LUNs** e, em seguida, clique no volume ou nome LUN desejado.
2. Clique Protect em .
3. Selecione o cluster de destino e a VM de armazenamento.
4. A política assíncrona é selecionada por padrão. Para selecionar uma política síncrona, clique em **mais opções**.
5. Clique em **Protect**.
6. Clique na guia **SnapMirror (local ou remoto)** para o volume ou LUN selecionado para verificar se a proteção está configurada corretamente.

CLI

1. No cluster de destino, crie uma relação de replicação:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   O `schedule` parâmetro não é aplicável ao criar relações síncronas do SnapMirror.

   O exemplo a seguir cria uma relação de DR do SnapMirror usando a política padrão `MirrorLatest`:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   O exemplo a seguir cria um relacionamento SnapVault usando a política padrão `XDPDefault`:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   O exemplo a seguir cria uma relação de replicação unificada usando a política padrão `MirrorAndVault`:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorAndVault
```

O exemplo a seguir cria uma relação de replicação unificada usando a política personalizada `my_unified`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

O exemplo a seguir cria um relacionamento síncrono do SnapMirror usando a política padrão `Sync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

O exemplo a seguir cria um relacionamento síncrono do SnapMirror usando a política padrão `StrictSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

O exemplo a seguir cria uma relação de DR do SnapMirror. Com o tipo DP convertido automaticamente para XDP e sem nenhuma política especificada, a política é padrão para a `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

O exemplo a seguir cria uma relação de DR do SnapMirror. Sem nenhum tipo ou política especificada, a política é padrão para a `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

O exemplo a seguir cria uma relação de DR do SnapMirror. Sem nenhuma política especificada, a política é padrão para a `XDPDefault` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

O exemplo a seguir cria um relacionamento síncrono do SnapMirror com a política `SnapCenterSync`predefinida :

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

A política predefinida `SnapCenterSync` é do tipo `Sync`. Essa política replica qualquer cópia Snapshot criada com o `snapmirror-label` de "app_consistent".

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Informações relacionadas

- "Criar e excluir volumes de teste de failover do SnapMirror".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral do backup de volume usando o SnapVault"

Inicializar uma relação de replicação

Para todos os tipos de relacionamento, a inicialização executa uma *Baseline transfer*: Ele faz uma cópia Snapshot do volume de origem, depois transfere essa cópia e todos os blocos de dados que ela faz referência ao volume de destino. Caso contrário, o conteúdo da transferência depende da política.

O que você vai precisar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

"Peering de cluster e SVM"

Sobre esta tarefa

A inicialização pode ser demorada. Você pode querer executar a transferência de linha de base em horas fora do pico.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas.

Passo

1. Inicializar uma relação de replicação:

   ```
   snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir inicializa a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Exemplo: Configurar uma cascata Vault-Vault

Um exemplo mostrará em termos concretos como você pode configurar relacionamentos de replicação uma etapa de cada vez. Você pode usar a implantação em cascata do Vault-Vault configurada no exemplo para reter mais de 251 cópias Snapshot rotuladas "semanal".

O que você vai precisar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.
- Você deve estar executando o ONTAP 9.2 ou posterior. As cascatas do Vault-Vault não são suportadas em versões anteriores do ONTAP.

Sobre esta tarefa

O exemplo assume o seguinte:

- Você configurou cópias Snapshot no cluster de origem com os rótulos SnapMirror """diariamente", "semanal" e "mensal".
- Você configurou volumes de destino chamados "volA" nos clusters de destino secundário e terciário.
- Você configurou as programações de tarefas de replicação chamadas "mmy_SnapVault" nos clusters de destino secundário e terciário.

O exemplo mostra como criar relacionamentos de replicação com base em duas políticas personalizadas:

- A política "SnapVault_secondary" retém 7 cópias Snapshot diárias, 52 semanais e 180 mensais no cluster de destino secundário.
- A política SnapVault_terciária mantém 250 cópias Snapshot semanais no cluster de destino terciário.

Passos

1. No cluster de destino secundário, crie a política "SnapVault_secondary":

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment “Policy on secondary for vault to vault cascade” -vserver
   svm_secondary
   ```

2. No cluster de destino secundário, defina a regra "diariamente" para a política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. No cluster de destino secundário, defina a regra "semanal" para a política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. No cluster de destino secundário, defina a regra "mensal" para a política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. No cluster de destino secundário, verifique a política:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily               7  false       0 -
-
                              my-weekly             52  false       0 -
-
                              my-monthly           180  false       0 -
-
```

6. No cluster de destino secundário, crie a relação com o cluster de origem:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. No cluster de destino secundário, inicialize a relação com o cluster de origem:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. No cluster de destino terciário, crie a política "'SnapVault_terciária":

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment “Policy on tertiary for vault to vault cascade” -vserver
svm_tertiary
```

9. No cluster de destino terciário, defina a regra "semanal" para a política:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. No cluster de destino terciário, verifique a política:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. No cluster de destino terciário, crie a relação com o cluster secundário:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. No cluster de destino terciário, inicialize a relação com o cluster secundário:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Converta uma relação de tipo DP existente para XDP no ONTAP

Se você estiver atualizando para o ONTAP 9.12,1 ou posterior, você deverá converter relações do tipo DP para XDP antes de atualizar. O ONTAP 9.12,1 e posterior não suporta relações do tipo DP. Você pode facilmente converter uma relação de tipo DP existente para XDP para aproveitar o SnapMirror flexível de versão.

Sobre esta tarefa

- O SnapMirror não converte automaticamente relacionamentos do tipo DP existentes para XDP. Para converter o relacionamento, você precisa quebrar e excluir o relacionamento existente, criar um novo relacionamento XDP e ressincronizar o relacionamento. Para obter informações de fundo, "O XDP substitui o DP como o padrão SnapMirror"consulte .
- Ao Planejar sua conversão, você deve estar ciente de que a preparação em segundo plano e a fase de armazenamento de dados de um relacionamento XDP SnapMirror podem levar muito tempo. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

> Depois de converter um tipo de relacionamento SnapMirror de DP para XDP, as configurações relacionadas ao espaço, como dimensionamento automático e garantia de espaço, não são mais replicadas para o destino.

Passos

1. No cluster de destino, verifique se a relação SnapMirror é do tipo DP, se o estado do espelho é SnapMirrored, o status do relacionamento está ocioso e se o relacionamento está saudável:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   O exemplo a seguir mostra a saída do `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

Você pode achar útil manter uma cópia da[`snapmirror show` saída do comando para manter o controle existente das configurações de relacionamento. Saiba mais sobre o comando `snapmirror show` na referência de comando ONTAP.

2. A partir dos volumes de origem e destino, verifique se ambos os volumes têm uma cópia Snapshot comum:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra a `volume snapshot show` saída para os volumes de origem e destino:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantir que as atualizações agendadas não sejam executadas durante a conversão, execute o relacionamento existente do tipo DP:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-quiesce.html[`snapmirror quiesce`(em inglês) na referência de comando ONTAP.

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir anula a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` em `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Quebre a relação existente do tipo DP:

```
snapmirror break -destination-path <SVM:volume>
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-break.html[`snapmirror-break`(em inglês) na referência de comando ONTAP .

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir rompe a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Se a exclusão automática de cópias Snapshot estiver ativada no volume de destino, desative-a:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

O exemplo a seguir desativa a cópia snapshot autodelete no volume de `volA_dst` destino :

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Eliminar a relação do tipo DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-delete.html[`snapmirror-delete`(em inglês) na referência de comando ONTAP.

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir exclui a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Solte a relação de recuperação de desastres do SVM de origem na fonte:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

O exemplo a seguir libera a relação de recuperação de desastres da SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. Você pode usar a saída que reteve do `snapmirror show` comando para criar a nova relação do tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

O novo relacionamento deve usar o mesmo volume de origem e destino. Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir cria uma relação de recuperação de desastres do SnapMirror entre o volume de origem `volA` ligado `svm1` e o volume de `volA_dst` destino ligado `svm_backup` usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Ressincronizar os volumes de origem e destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para melhorar o tempo de ressincronização, você pode usar a `-quick-resync` opção, mas deve estar ciente de que a economia com eficiência de storage pode ser perdida. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/SnapMirror-resync.html n.o parameters.html[`snapmirror resync` na referência de comando ONTAP.

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Se a exclusão automática de cópias Snapshot for desativada, reative-a:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Depois de terminar

1. Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada.
2. Quando o volume de destino XDP do SnapMirror começar a atualizar cópias Snapshot conforme definido pela política SnapMirror, use a saída `snapmirror list-destinations` do comando do cluster de origem para exibir a nova relação XDP do SnapMirror.

Converta o tipo de uma relação SnapMirror

A partir do ONTAP 9.5, o SnapMirror síncrono é suportado. Você pode converter uma relação assíncrona do SnapMirror para uma relação síncrona do SnapMirror ou vice-versa sem realizar uma transferência de linha de base.

Sobre esta tarefa

Não é possível converter uma relação assíncrona do SnapMirror para uma relação síncrona do SnapMirror ou vice-versa alterando a política do SnapMirror

Passos

- * Conversão de uma relação assíncrona do SnapMirror para uma relação síncrona do SnapMirror*

  a. No cluster de destino, exclua a relação assíncrona do SnapMirror:

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

b. No cluster de origem, libere a relação do SnapMirror sem excluir as cópias Snapshot comuns:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. No cluster de destino, crie uma relação síncrona SnapMirror:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM>:<destination_volume> -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. Ressincronizar a relação síncrona do SnapMirror:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- * Conversão de uma relação síncrona SnapMirror para uma relação assíncrona SnapMirror*

a. A partir do cluster de destino, quiesce a relação síncrona SnapMirror existente:

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. No cluster de destino, exclua a relação assíncrona do SnapMirror:

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. No cluster de origem, libere a relação do SnapMirror sem excluir as cópias Snapshot comuns:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. No cluster de destino, crie uma relação assíncrona do SnapMirror:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Ressincronizar a relação síncrona do SnapMirror:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Converta o modo de uma relação síncrona SnapMirror

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas. Você pode converter o modo de uma relação síncrona SnapMirror de StrictSync para sincronização ou vice-versa.

Sobre esta tarefa

Você não pode modificar a política de uma relação síncrona SnapMirror para converter seu modo.

Passos

1. A partir do cluster de destino, quiesce a relação síncrona SnapMirror existente:

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. No cluster de destino, exclua a relação síncrona SnapMirror existente:

```
snapmirror delete -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. No cluster de origem, libere a relação do SnapMirror sem excluir as cópias Snapshot comuns:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. No cluster de destino, crie uma relação síncrona SnapMirror especificando o modo para o qual você deseja converter a relação síncrona SnapMirror:

   ```
   snapmirror create -source-path vs1:vol1 -destination-path
   <destination_SVM>:<destination_volume> -policy Sync|StrictSync
   ```

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. A partir do cluster de destino, ressincronize a relação SnapMirror:

   ```
   snapmirror resync -destination-path <destination_SVM>:<destination_volume>
   ```

   ```
   cluster2::> snapmirror resync -destination-path vs1_dr:vol1
   ```

Criar e excluir volumes de teste de failover do SnapMirror

A partir do ONTAP 9.14,1, você pode usar o System Manager para criar um clone de volume para testar o failover do SnapMirror e a recuperação de desastres sem interromper o relacionamento do SnapMirror ativo. Quando terminar o teste, você pode limpar os dados associados e excluir o volume do teste.

Criar um volume de teste de failover do SnapMirror

Sobre esta tarefa

- É possível executar testes de failover em relacionamentos assíncronos e assíncronos do SnapMirror.
- Um clone de volume é criado para executar o teste de recuperação de desastre.
- O volume do clone é criado na mesma VM de storage que o destino do SnapMirror.
- Você pode usar relacionamentos FlexVol e FlexGroup SnapMirror.
- Se já existir um clone de teste para a relação selecionada, não é possível criar outro clone para essa relação.
- As relações do SnapLock Vault não são suportadas.

Antes de começar

- Você deve ser um administrador de cluster.
- A licença SnapMirror deve ser instalada no cluster de origem e destino.

Passos

1. No cluster de destino, selecione **proteção > relacionamentos**.
2. Selecione ⋮ ao lado da fonte do relacionamento e escolha **Teste failover**.

3. Na janela **Teste failover**, selecione **Teste failover**.
4. Selecione **Storage > volumes** e verifique se o volume de failover de teste está listado.
5. Selecione **armazenamento > partilhar**.
6. Clique  e escolha **compartilhar**.
7. Na janela **Adicionar compartilhamento**, digite um nome para o compartilhamento no campo **Nome do compartilhamento**.
8. No campo **pasta**, selecione **Procurar**, selecione o volume do clone de teste e **Salvar**.
9. Na parte inferior da janela **Adicionar compartilhamento**, escolha **Salvar**.
10. Abra o compartilhamento no cliente e verifique se o volume de teste tem recursos de leitura e gravação.

Limpe os dados de failover e exclua o volume de teste

Depois de concluir o teste de failover, você pode limpar todos os dados associados ao volume de teste e excluí-lo.

Passos

1. No cluster de destino, selecione **proteção > relacionamentos**.
2. Selecione ⋮ ao lado da fonte do relacionamento e escolha **Limpar failover de teste**.
3. Na janela **Limpar failover de teste**, selecione **Limpar**.
4. Selecione **armazenamento > volumes** e verifique se o volume de teste foi excluído.

Fornecer dados de um volume de destino do SnapMirror DR

Torne o volume de destino gravável

Você precisa fazer com que o volume de destino seja gravável antes de poder fornecer dados do volume para os clientes. Para servir dados de um destino espelhado quando uma origem ficar indisponível, pare as transferências agendadas para o destino e, em seguida, quebre a relação SnapMirror para tornar o destino gravável.

Sobre esta tarefa

É necessário executar essa tarefa a partir do SVM de destino ou do cluster de destino.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para tornar um volume de destino gravável.

System Manager

1. Selecione a relação de proteção: Clique em **proteção > relacionamentos** e, em seguida, clique no nome do volume desejado.
2. Clique em .
3. Parar transferências agendadas : clique em **Pausar**.
4. Deixe o destino gravável: Clique em **Break**.
5. Vá para a página principal **relacionamentos** para verificar se o estado da relação é exibido como "quebrado".

Próximas etapas

Você precisa "ressincronizar a relação de replicação reversa" depois de fazer um volume de destino gravável.

Quando o volume de origem desativado estiver novamente disponível, você deverá voltar a sincronizar a relação novamente para copiar os dados atuais para o volume de origem original.

CLI

1. Parar transferências programadas para o destino:

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir interrompe as transferências agendadas entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

2. Parar transferências contínuas para o destino:

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

   Para obter a sintaxe completa do comando, consulte a página man.

   Esta etapa não é necessária para relacionamentos síncronos do SnapMirror (suportado a partir do ONTAP 9.5).

   O exemplo a seguir interrompe as transferências contínuas entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

3. Quebre a relação de DR do SnapMirror:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir rompe a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` no `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Próximas etapas

Você precisa "ressincronize a relação de replicação" depois de fazer um volume de destino gravável.

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da recuperação de desastres de volume"

Configure o volume de destino para acesso aos dados

Depois de fazer o volume de destino gravável, você deve configurar o volume para acesso aos dados. Clientes nas, subsistema NVMe e hosts SAN podem acessar os dados do volume de destino até que o volume de origem seja reativado.

Ambiente nas:

1. Monte o volume nas no namespace usando o mesmo caminho de junção no qual o volume de origem foi montado no SVM de origem.
2. Aplique as ACLs apropriadas aos compartilhamentos SMB no volume de destino.
3. Atribua as políticas de exportação NFS ao volume de destino.
4. Aplique as regras de quota ao volume de destino.
5. Redirecione os clientes para o volume de destino.
6. Remontagem dos compartilhamentos de NFS e SMB nos clientes.

AMBIENTE SAN:

1. Mapeie os LUNs no volume para o grupo de iniciadores apropriado.
2. Para iSCSI, crie sessões iSCSI dos iniciadores do host SAN para os LIFs SAN.
3. No cliente SAN, efetue uma nova verificação de armazenamento para detetar os LUNs ligados.

Para obter informações sobre o ambiente NVMe, "Administração da SAN"consulte .

Reative o volume da fonte original

É possível restabelecer a relação de proteção de dados original entre os volumes de origem e destino quando não precisar mais fornecer dados do destino.

Sobre esta tarefa

- O procedimento abaixo pressupõe que a linha de base no volume de origem original está intacta. Se a linha de base não estiver intacta, você deverá criar e inicializar a relação entre o volume do qual você está fornecendo dados e o volume de origem original antes de executar o procedimento.
- A preparação em segundo plano e a fase de armazenamento de dados de um relacionamento XDP SnapMirror podem levar muito tempo. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

Passos

1. Inverta a relação original de proteção de dados:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original. Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico. O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. `snapmirror initialize`Use para reinicializar o relacionamento.

   O exemplo a seguir inverte a relação entre o volume de origem original, `volA` On (ligado `svm1`) e o volume do qual você está fornecendo dados, `volA_dst` On (ligado `svm_backup`):

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. Quando estiver pronto para restabelecer o acesso aos dados à origem original, pare o acesso ao volume de destino original. Uma maneira de fazer isso é parar o SVM de destino original:

   `vserver stop -vserver` *`SVM`*

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir do SVM de destino original ou do cluster de destino original. Esse comando interrompe o acesso do usuário a todo o SVM de destino original. Pode pretender parar o acesso ao volume de destino original utilizando outros métodos.

O exemplo a seguir interrompe o SVM de destino original:

```
cluster_dst::> vserver stop svm_backup
```

3. Atualize a relação invertida:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

   O exemplo a seguir atualiza a relação entre o volume do qual você está fornecendo dados, `volA_dst` ligado `svm_backup` e o volume de origem original, `volA` ligado `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

4. A partir do SVM de origem original ou do cluster de origem original, interrompa as transferências agendadas do relacionamento invertido:

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

   O exemplo a seguir interrompe as transferências agendadas entre o volume de destino original, `volA_dst` On (ligado `svm_backup`) e o volume de origem original `volA`, On (ligado `svm1`):

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

5. Quando a atualização final estiver concluída e o relacionamento indicar "Quiesced" para o status do relacionamento, execute o seguinte comando da fonte original SVM ou do cluster de origem original para quebrar o relacionamento invertido::

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem.

   O exemplo a seguir rompe a relação entre o volume de destino original, `volA_dst` ligado `svm_backup` e o volume de origem original, `volA` ligado `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. No SVM de origem original ou no cluster de origem original, exclua a relação de proteção de dados invertida:

   `snapmirror delete -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

   O exemplo a seguir exclui a relação inversa entre o volume de origem original, `volA` ligado `svm1` e o volume do qual você está fornecendo dados, `volA_dst` ligado `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Liberar a relação inversa do SVM de destino original ou do cluster de destino original.

   `snapmirror release -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > Você deve executar esse comando a partir do SVM de destino original ou do cluster de destino original.

   O exemplo a seguir libera a relação inversa entre o volume de destino original, `volA_dst` On (ligado `svm_backup`) e o volume de origem original `volA`, On (ligado `svm1`):

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Restabelecer a relação de proteção de dados original a partir do destino original:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir restabelece a relação entre o volume de origem original, `volA` ligado `svm1` e o volume de destino original `volA_dst`, ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Se necessário, inicie o SVM de destino original:

`vserver start -vserver SVM`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir inicia o SVM de destino original:

```
cluster_dst::> vserver start svm_backup
```

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Restaure arquivos de um volume de destino do SnapMirror

Restaure um único namespace de arquivo, LUN ou NVMe a partir de um destino do SnapMirror

É possível restaurar um único arquivo, LUN, um conjunto de arquivos ou LUNs de uma cópia Snapshot ou um namespace NVMe a partir de um volume de destino do SnapMirror. A partir do ONTAP 9.7, você também pode restaurar namespaces NVMe a partir de um destino síncrono SnapMirror. Pode restaurar ficheiros para o volume de origem original ou para um volume diferente.

O que você vai precisar

Para restaurar um arquivo ou LUN de um destino síncrono SnapMirror (suportado a partir do ONTAP 9.5), primeiro você deve excluir e liberar a relação.

Sobre esta tarefa

O volume para o qual você está restaurando arquivos ou LUNs (o volume de destino) deve ser um volume de leitura e gravação:

- O SnapMirror executa uma *restauração incremental* se os volumes de origem e destino tiverem uma cópia Snapshot comum (como é normalmente o caso quando você está restaurando para o volume de origem original).
- Caso contrário, o SnapMirror executa uma *restauração de linha de base*, na qual a cópia Snapshot especificada e todos os blocos de dados que ele faz referência são transferidos para o volume de destino.

Passos

1. Listar as cópias Snapshot no volume de destino:

   `volume snapshot show -vserver <SVM> -volume volume`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir mostra as cópias Snapshot `vserverB:secondary1` no destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure um único arquivo ou LUN ou um conjunto de arquivos ou LUNs de uma cópia Snapshot em um volume de destino do SnapMirror:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot -file-list <source_file_path,@destination_file_path>
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

   O comando a seguir restaura os `file1` arquivos e `file2` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` , para o mesmo local no sistema de arquivos ativo do volume de origem original `primary1` :

   ```
   cluster_dst::> snapmirror restore -source-path vserverB:secondary1
   -destination-path vserverA:primary1 -source-snapshot daily.2013-01-
   25_0010 -file-list /dir1/file1,/dir2/file2

   [Job 3479] Job is queued: snapmirror restore for the relationship with
   destination vserverA:primary1
   ```

O comando a seguir restaura os `file1` arquivos e `file2` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` para um local diferente no sistema de arquivos ativo do volume de origem original `primary1` .

O caminho do arquivo de destino começa com o símbolo at seguido pelo caminho do arquivo a partir da raiz do volume de origem original. Neste exemplo, `file1` é restaurado para `/dir1/file1.new` e file2 é restaurado para `/dir2.new/file2` ON `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

O comando a seguir restaura os `file1` arquivos e `file3` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` , para diferentes locais no sistema de arquivos ativo do volume de origem original `primary1` e restaura `file2` de `snap1` para o mesmo local no sistema de arquivos ativo `primary1` do .

Neste exemplo, o arquivo `file1` é restaurado para `/dir1/file1.new` e `file3` é restaurado para `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Restaure o conteúdo de um volume a partir de um destino SnapMirror

É possível restaurar o conteúdo de um volume inteiro a partir de uma cópia Snapshot em um volume de destino do SnapMirror. Pode restaurar o conteúdo do volume para o volume de origem original ou para um volume diferente.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para restaurar os dados. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

O volume de destino para a operação de restauração deve ser um dos seguintes:

- Um volume de leitura e gravação, nesse caso, o SnapMirror executa uma *restauração incremental*, desde que os volumes de origem e destino tenham uma cópia Snapshot comum (como normalmente ocorre

quando você está restaurando para o volume de origem original).

> O comando falhará se não houver uma cópia Snapshot comum. Não é possível restaurar o conteúdo de um volume para um volume de leitura e gravação vazio.

- Um volume de proteção de dados vazio, nesse caso, o SnapMirror executa uma *restauração de linha de base*, na qual a cópia Snapshot especificada e todos os blocos de dados que ele faz referência são transferidos para o volume de origem.

Restaurar o conteúdo de um volume é uma operação disruptiva. O tráfego SMB não deve estar em execução no volume primário do SnapVault quando uma operação de restauração está em execução.

Se o volume de destino para a operação de restauração tiver a compactação ativada e o volume de origem não tiver a compactação ativada, desative a compactação no volume de destino. Você precisa reativar a compactação após a conclusão da operação de restauração.

Todas as regras de quota definidas para o volume de destino são desativadas antes de a restauração ser executada. Você pode usar o `volume quota modify` comando para reativar regras de cota após a conclusão da operação de restauração.

Quando os dados em um volume são perdidos ou corrompidos, você pode reverter seus dados restaurando a partir de uma cópia Snapshot anterior.

Este procedimento substitui os dados atuais no volume de origem por dados de uma versão anterior da cópia Snapshot. Deve executar esta tarefa no cluster de destino.

Passos

Você pode restaurar o conteúdo de um volume usando o Gerenciador do sistema ou a CLI do ONTAP.

System Manager

1. Clique em **proteção > relacionamentos** e, em seguida, clique no nome do volume de origem.
2. Clique em e selecione **Restore**.
3. Em **fonte**, o volume da fonte é selecionado por padrão. Clique em **outro volume** se quiser escolher um volume diferente da origem.
4. Em **destino**, escolha a cópia Snapshot que deseja restaurar.
5. Se a origem e o destino estiverem localizados em clusters diferentes, no cluster remoto, clique em **proteção > relacionamentos** para monitorar o progresso da restauração.

CLI

1. Listar as cópias Snapshot no volume de destino:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra as cópias Snapshot `vserverB:secondary1` no destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure o conteúdo de um volume a partir de uma cópia Snapshot em um volume de destino do SnapMirror:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

Para obter a sintaxe completa do comando, consulte a página man.

> Você deve executar esse comando a partir da fonte original SVM ou do cluster de origem original.

O comando a seguir restaura o conteúdo do volume de origem original `primary1` da cópia Snapshot `daily.2013-01-25_0010` no volume de destino original `secondary1` :

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Remonte o volume restaurado e reinicie todos os aplicativos que usam o volume.

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Restauração de volume usando visão geral do SnapVault"

Atualizar uma relação de replicação manualmente

Talvez seja necessário atualizar manualmente uma relação de replicação se uma atualização falhar porque o volume de origem foi movido.

Sobre esta tarefa

O SnapMirror aborta quaisquer transferências de um volume de origem movido até que você atualize a relação de replicação manualmente.

A partir do ONTAP 9.5, as relações síncronas do SnapMirror são suportadas. Embora os volumes de origem e destino estejam sempre sincronizados nessas relações, a exibição do cluster secundário é sincronizada com o primário apenas por hora. Se você quiser exibir os dados pontuais no destino, você deve executar uma atualização manual executando o `snapmirror update` comando.

Passo

1. Atualizar manualmente uma relação de replicação:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. `snapmirror initialize`Use para reinicializar o relacionamento.

   O exemplo a seguir atualiza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Ressincronizar uma relação de replicação

É necessário ressincronizar uma relação de replicação depois de fazer um volume de destino gravável, depois de uma atualização falhar porque uma cópia Snapshot comum não existe nos volumes de origem e destino ou se você quiser alterar a política de replicação para a relação.

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para executar uma operação de ressincronização reversa para excluir uma relação de proteção existente e reverter as funções dos volumes de origem e destino. Em seguida, você usa o volume de destino para servir dados enquanto você reparar ou substituir a origem, atualizar a origem e restabelecer a configuração original dos sistemas.

Sobre esta tarefa

- Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.
- Os volumes que fazem parte de uma configuração de fan-out ou cascata podem levar mais tempo para ressincronizar. Não é incomum ver a relação do SnapMirror informando o status "preparando" por um período de tempo prolongado.

> O System Manager não é compatível com a ressincronização reversa com relacionamentos entre clusters. Você pode usar a CLI do ONTAP para realizar operações ressincronizadas revertidas com relacionamentos entre clusters.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para executar esta tarefa. Se você usar a CLI do ONTAP, o procedimento será o mesmo, independentemente de você estar criando um volume de destino gravável ou atualizando a relação de replicação.

Ressincronização reversa do System Manager

Depois de "quebre um relacionamento"fazer um destino gravável, volte a sincronizar a relação:

1. No cluster de destino, clique em **proteção > relacionamentos**.
2. Passe o Mouse sobre a relação quebrada que você deseja reverter, clique em e selecione **Reverse Resync**.
3. Na janela **Reverse Resync relation**, clique em **Reverse Resync**.
4. Em **relacionamentos**, monitore o progresso da ressincronização reversa visualizando **Status da transferência** para o relacionamento.

Próximas etapas

Quando a fonte original estiver disponível novamente, você poderá restabelecer a relação original quebrando a relação invertida e realizando outra operação ressincronizada reversa. O processo de ressincronização reversa copiará todas as alterações do site que está fornecendo dados para a fonte original e fará a fonte original ler-gravável novamente.

Ressincronizar o System Manager

1. Clique em **proteção > relacionamentos**.
2. Passe o Mouse sobre o relacionamento que você deseja ressincronizar e clique e selecione **Break**.
3. Quando o estado do relacionamento exibir "desagregado", clique e selecione **Resync**.
4. Em **relacionamentos**, monitore o progresso da ressincronização verificando o estado do relacionamento. O estado muda para "espelhado" quando a ressincronização é concluída.

CLI

1. Ressincronizar os volumes de origem e destino:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

Para obter a sintaxe completa do comando, consulte a página man.

> Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de `volA_dst` destino ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Excluir uma relação de replicação de volume

Você pode usar os `snapmirror delete` comandos e `snapmirror release` para excluir uma relação de replicação de volume. Em seguida, pode eliminar manualmente volumes de destino desnecessários.

Sobre esta tarefa

```
`snapmirror release`O comando exclui todas as cópias Snapshot criadas pelo
SnapMirror da origem. Você pode usar a `-relationship-info-only` opção
para preservar as cópias Snapshot.
```

Passos

1. Quiesce a relação de replicação:

   ```
   snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>
   ```

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

2. (Opcional) quebre a relação de replicação se você precisar que o volume de destino seja um volume de leitura/gravação. Pode ignorar esta etapa se pretender eliminar o volume de destino ou se não necessitar de ler/escrever o volume:

   ```
   snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

3. Eliminar a relação de replicação:

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   Você deve executar esse comando a partir do cluster de destino ou SVM de destino.

   O exemplo a seguir exclui a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA_dst` ligado `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

4. Liberar informações de relação de replicação da fonte SVM:

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

Para obter a sintaxe completa do comando, consulte a página man.

Você deve executar esse comando a partir do cluster de origem ou da SVM de origem.

O exemplo a seguir libera informações para a relação de replicação especificada da SVM de origem `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Gerenciar a eficiência de storage

O SnapMirror preserva a eficiência de storage nos volumes de origem e destino, exceto quando a compactação de dados pós-processamento está ativada no volume de destino. Nesse caso, toda a eficiência de storage é perdida no volume de destino. Para corrigir esse problema, você precisa desativar a compactação pós-processo no volume de destino, atualizar a relação manualmente e reativar a eficiência de storage.

Sobre esta tarefa

Você pode usar o `volume efficiency show` comando para determinar se a eficiência está ativada em um volume. Para obter mais informações, consulte as páginas de manual.

Você pode verificar se o SnapMirror está mantendo a eficiência de storage visualizando os logs de auditoria do SnapMirror e localizando a descrição da transferência. Se a descrição da transferência for exibida `transfer_desc=Logical Transfer with Storage Efficiency`, o SnapMirror manterá a eficiência do storage. Se a descrição da transferência for exibida `transfer_desc=Logical Transfer`, o SnapMirror não manterá a eficiência do storage. Por exemplo:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Antes de começar

- Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

  "Peering de cluster e SVM"

- Você deve desativar a compressão pós-processo no volume de destino.
- Transferência lógica com armazenamento: A partir do ONTAP 9.3, a atualização manual não é mais necessária para reativar a eficiência de storage. Se o SnapMirror detetar que a compactação pós-processo foi desativada, ele reativará automaticamente a eficiência de storage na próxima atualização

agendada. Tanto a origem quanto o destino devem estar executando o ONTAP 9.3.

- A partir do ONTAP 9.3, os sistemas AFF gerenciam as configurações de eficiência de storage de maneira diferente dos sistemas FAS depois que um volume de destino é gravado:
  - Depois de fazer um volume de destino gravável usando o `snapmirror break` comando, a política de cache no volume é automaticamente definida como "'auto'" (o padrão).

    Esse comportamento é aplicável apenas a volumes do FlexVol e não se aplica a volumes do FlexGroup.

  - Na ressincronização, a política de armazenamento em cache é automaticamente definida como "nenhum", e a deduplicação e a compactação in-line são desativadas automaticamente, independentemente das configurações originais. Você deve modificar as configurações manualmente, conforme necessário.

Atualizações manuais com eficiência de storage habilitada podem ser demoradas. Você pode querer executar a operação em horas fora do pico.

Passos

1. Atualizar uma relação de replicação e reativar a eficiência de storage:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

Para obter a sintaxe completa do comando, consulte a página man.

Você deve executar esse comando a partir do SVM de destino ou do cluster de destino. O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. `snapmirror initialize`Use para reinicializar o relacionamento.

O exemplo a seguir atualiza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino ligado `svm_backup` e `volA_dst` rehabilita a eficiência de storage:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Use a regulagem global do SnapMirror

A regulagem global da rede está disponível para todas as transferências SnapMirror e SnapVault em um nível por nó.

Sobre esta tarefa

A regulagem global da SnapMirror restringe a largura de banda usada pelas transferências SnapMirror e SnapVault de entrada e/ou saída. A restrição é aplicada em todo o cluster em todos os nós no cluster.

Por exemplo, se o acelerador de saída estiver definido para 100 Mbps, cada nó no cluster terá a largura de

banda de saída definida para 100 Mbps. Se a limitação global estiver desativada, ela será desativada em todos os nós.

Embora as taxas de transferência de dados sejam frequentemente expressas em bits por segundo (bps), os valores do acelerador devem ser inseridos em kilobytes por segundo (kbps).

> No ONTAP 9.9,1 e versões anteriores, o acelerador não tem efeito em `volume move` transferências ou transferências de espelho de compartilhamento de carga. Começando com ONTAP 9.10,0, você pode especificar uma opção para controlar as operações de movimentação de volume. Para obter detalhes, consulte "Como mover o volume do acelerador em ONTAP 9.10 e mais tarde."

A regulagem global funciona com o recurso de aceleração por relacionamento para transferências SnapMirror e SnapVault. O acelerador por relação é aplicado até que a largura de banda combinada de transferências por relação exceda o valor do acelerador global, após o qual o acelerador global é aplicado. Um valor de aceleração `0` implica que a limitação global está desativada.

> A regulagem global do SnapMirror não tem efeito nas relações síncronas do SnapMirror quando elas estão em sincronia. No entanto, o acelerador afeta as relações síncronas do SnapMirror quando executam uma fase de transferência assíncrona, como uma operação de inicialização ou após um evento fora de sincronização. Por esse motivo, não é recomendável habilitar a limitação global com relacionamentos síncronos do SnapMirror.

Passos

1. Ativar a limitação global:

   `options -option-name replication.throttle.enable on|off`

   O exemplo a seguir mostra como ativar a limitação global do SnapMirror no `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Especifique a largura de banda total máxima usada pelas transferências recebidas no cluster de destino:

   `options -option-name replication.throttle.incoming.max_kbs` *KBps*

   A largura de banda mínima recomendada do acelerador é de 4 kbps e o máximo é de até 2 Tbps. O valor padrão para essa opção é `unlimited`, o que significa que não há limite na largura de banda total usada.

   O exemplo a seguir mostra como definir a largura de banda total máxima usada pelas transferências recebidas para 100 Mbps:

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 Mbps: 12500 kbps

3. Especifique a largura de banda total máxima utilizada pelas transferências efetuadas no cluster de origem:

`options -option-name replication.throttle.outgoing.max_kbs KBps`

A largura de banda mínima recomendada do acelerador é de 4 kbps e o máximo é de até 2 Tbps. O valor padrão para essa opção é `unlimited`, o que significa que não há limite na largura de banda total usada. Os valores dos parâmetros estão em kbps.

O exemplo a seguir mostra como definir a largura de banda total máxima usada pelas transferências de saída para 100 Mbps:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Gerenciar a replicação do SnapMirror SVM

Saiba mais sobre a replicação do ONTAP SnapMirror SVM

Você pode usar o SnapMirror para criar uma relação de proteção de dados entre SVMs. Nesse tipo de relação, toda ou parte da configuração do SVM, de exportações de NFS e compartilhamentos de SMB a RBAC, são replicados, bem como os dados nos volumes proprietários do SVM.

Tipos de relacionamento suportados

Somente SVMs de fornecimento de dados podem ser replicadas. Os seguintes tipos de relacionamento de proteção de dados são compatíveis:

- *SnapMirror DR,* no qual o destino normalmente contém apenas as cópias Snapshot atualmente na origem.

  A partir do ONTAP 9.9,1, esse comportamento muda quando você está usando a política mirror-Vault. A partir do ONTAP 9.9,1, você pode criar diferentes políticas de Snapshot na origem e no destino. Além disso, as cópias snapshot no destino não são sobrescritas por cópias Snapshot na origem:

  - Eles não são sobrescritos da origem para o destino durante operações normais agendadas, atualizações e ressincronização
  - Eles não são excluídos durante operações de interrupção.
  - Eles não são excluídos durante operações flip-ressync. Quando você configura um relacionamento de desastre SVM usando a política de espelhamento de arquivos usando o ONTAP 9.9,1 e posterior, a política se comporta da seguinte forma:
  - As políticas de cópia Snapshot definidas pelo usuário na origem não são copiadas para o destino.
  - As políticas de cópia Snapshot definidas pelo sistema não são copiadas para o destino.
  - A associação de volume com políticas Snapshot definidas pelo usuário e pelo sistema não é copiada para o destino. COM SVM.
- A partir do ONTAP 9.2, *replicação unificada do SnapMirror,* na qual o destino é configurado para DR e retenção de longo prazo.

Para obter mais informações sobre a replicação unificada do SnapMirror, "Noções básicas de replicação unificada da SnapMirror"consulte .

O *policy type* da diretiva de replicação determina o tipo de relação que ela suporta. A tabela a seguir mostra os tipos de diretiva disponíveis.

Tipo de política	Tipo de relação
espelho assíncrono	SnapMirror DR
espelho-cofre	Replicação unificada

O XDP substitui o DP como o padrão de replicação SVM no ONTAP 9.4

A partir do ONTAP 9.4, as relações de proteção de dados do SVM passam por padrão no modo XDP. As relações de proteção de dados do SVM continuam como padrão no modo DP no ONTAP 9.3 e versões anteriores.

Relacionamentos existentes não são afetados pelo novo padrão. Se uma relação já for do tipo DP, ela continuará sendo do tipo DP. A tabela a seguir mostra o comportamento que você pode esperar.

Se especificar…	O tipo é…	A política padrão (se você não especificar uma política) é…
DP	XDP	Espelhamento AllSnapshots (SnapMirror DR)
Nada	XDP	Espelhamento AllSnapshots (SnapMirror DR)
XDP	XDP	MirrorAndVault (replicação unificada)

Detalhes sobre as alterações no padrão podem ser encontrados aqui: "O XDP substitui o DP como o padrão SnapMirror".

> A independência de versão não é compatível com replicação SVM. Em uma configuração de recuperação de desastre do SVM, o SVM de destino deve estar em um cluster que executa a mesma versão de ONTAP do cluster de origem, para dar suporte a operações de failover e failback.

"Versões compatíveis do ONTAP para relacionamentos do SnapMirror"

Como as configurações da SVM são replicadas

O conteúdo de uma relação de replicação SVM é determinado pela interação dos seguintes campos:

- A `-identity-preserve true` opção `snapmirror create` do comando replica toda a configuração SVM.

  A `-identity-preserve false` opção replica apenas os volumes e as configurações de autenticação e autorização do SVM e as configurações de protocolo e serviço de nomes listadas em "Configurações replicadas em relacionamentos de recuperação de desastres da SVM".

- A `-discard-configs network` opção `snapmirror policy create` do comando exclui LIFs e configurações de rede relacionadas da replicação SVM, para uso nos casos em que as SVMs de origem e destino estão em sub-redes diferentes.
- A `-vserver-dr-protection unprotected` opção `volume modify` do comando exclui o volume especificado da replicação SVM.

Caso contrário, a replicação do SVM é quase idêntica à replicação de volume. Você pode usar praticamente o mesmo fluxo de trabalho para replicação de volume para SVM.

Detalhes do suporte

A tabela a seguir mostra os detalhes de suporte para replicação do SnapMirror SVM.

Recurso ou recurso	Detalhes do suporte
Tipos de implantação	• Origem única para destino único • Começando com ONTAP 9.4, fan-out. Você pode fazer fan-out apenas para dois destinos. Por padrão, somente um relacionamento verdadeiro que preserve identidade é permitido por SVM de origem.
Tipos de relacionamento	• Recuperação de desastres da SnapMirror • A partir do ONTAP 9.2, a replicação unificada do SnapMirror
Escopo de replicação	Apenas entre clusters. Não é possível replicar SVMs no mesmo cluster.
Proteção autônoma contra ransomware	• Suportado a partir de ONTAP 9.12,1. Para obter mais informações, "Proteção autônoma contra ransomware"consulte .
Grupos de consistência suporte assíncrono	A partir do ONTAP 9.14,1, há suporte para no máximo 32 relacionamentos de recuperação de desastres da SVM quando existem grupos de consistência. "Proteja um grupo de consistência"Consulte e "Limites do grupo de consistência" para obter mais informações.
FabricPool	A partir do ONTAP 9.6, a replicação do SnapMirror SVM é compatível com FabricPools.

MetroCluster	A partir do ONTAP 9.11,1, os dois lados de uma relação de recuperação de desastres do SVM em uma configuração MetroCluster podem funcionar como fonte de configurações adicionais de recuperação de desastres do SVM. A partir do ONTAP 9.5, a replicação do SnapMirror SVM é compatível com configurações do MetroCluster. • Em versões anteriores ao ONTAP 9.10.X, uma configuração do MetroCluster não pode ser o destino de uma relação de recuperação de desastres da SVM. • No ONTAP 9.10,1 e versões posteriores, uma configuração do MetroCluster pode ser o destino de uma relação de recuperação de desastres da SVM somente para fins de migração. Ela precisa atender a todos os requisitos necessários descritos na "TR-4966: Migração de um SVM para uma solução MetroCluster". • Somente um SVM ativo em uma configuração do MetroCluster pode ser a fonte de uma relação de recuperação de desastres do SVM. Uma fonte pode ser uma SVM de origem sincronizada antes do switchover ou um SVM de destino de sincronização após o switchover. • Quando uma configuração do MetroCluster está em um estado estável, o SVM de destino de sincronização do MetroCluster não pode ser a fonte de uma relação de recuperação de desastres do SVM, já que os volumes não estão online. • Quando o SVM de origem sincronizada é a fonte de uma relação de recuperação de desastres do SVM, as informações de origem no relacionamento de recuperação de desastres do SVM são replicadas para o parceiro MetroCluster. • Durante os processos de switchover e switchback, a replicação para o destino de recuperação de desastres da SVM pode falhar. No entanto, após a conclusão do processo de comutação ou switchback, as próximas atualizações agendadas de recuperação de desastres da SVM serão bem-sucedidas.

Grupo de consistência	Suportado a partir de ONTAP 9.14,1. Para obter mais informações, Proteja um grupo de consistênciaconsulte .
ONTAP S3	Não é compatível com recuperação de desastre do SVM.
SnapMirror síncrono	Não é compatível com recuperação de desastre do SVM.
Independência de versão	Não suportado.
Criptografia de volumes	• Volumes criptografados na origem são criptografados no destino. • Os servidores Onboard Key Manager ou KMIP devem ser configurados no destino. • Novas chaves de criptografia são geradas no destino. • Se o destino não contiver um nó que suporte a criptografia de volume .Encryption, a replicação será bem-sucedida, mas os volumes de destino não serão criptografados.

Configurações replicadas em relacionamentos de recuperação de desastres da SVM

A tabela a seguir mostra a interação `snapmirror create -identity-preserve` da opção e da `snapmirror policy create -discard-configs network` opção:

Configuração replicada		`-identity-preserve true`		`-identity-preserve false`
		Política sem `-discard -configs network` set	**Política com `-discard -configs network` SET**	
Rede	LIFs nas	Sim	Não	Não
Configuração do Kerberos LIF	Sim	Não	Não	SAN LIFs
Não	Não	Não	Políticas de firewall	Sim
Sim	Não	Políticas de serviço	Sim	Sim
Não	Rotas	Sim	Não	Não

Domínio de transmissão	Não	Não	Não	Sub-rede
Não	Não	Não	IPspace	Não
Não	Não	SMB	Servidor SMB	Sim
Sim	Não	Grupos locais e usuário local	Sim	Sim
Sim	Privilégio	Sim	Sim	Sim
Cópia de sombra	Sim	Sim	Sim	BranchCache
Sim	Sim	Sim	Opções de servidor	Sim
Sim	Sim	Segurança do servidor	Sim	Sim
Não	Diretório base, compartilhar	Sim	Sim	Sim
Link simbólico	Sim	Sim	Sim	Política de Fpolicy, Política de Fsecurity e Fsecurity NTFS
Sim	Sim	Sim	Mapeamento de nomes e mapeamento de grupos	Sim
Sim	Sim	Informações de auditoria	Sim	Sim
Sim	NFS	Políticas de exportação	Sim	Sim
Não	Regras de política de exportação	Sim	Sim	Não
Servidor NFS	Sim	Sim	Não	RBAC
Certificados de segurança	Sim	Sim	Não	Configuração de usuário de login, chave pública, função e função

Sim	Sim	Sim	SSL	Sim
Sim	Não	Serviços de nomes	DNS e DNS hosts	Sim
Sim	Não	Usuário UNIX e grupo UNIX	Sim	Sim
Sim	Kerberos Realm e blocos de chaves Kerberos	Sim	Sim	Não
Cliente LDAP e LDAP	Sim	Sim	Não	Grupo de rede
Sim	Sim	Não	NIS	Sim
Sim	Não	Acesso à Web e à Web	Sim	Sim
Não	Volume	Objeto	Sim	Sim
Sim	Cópias Snapshot e política do Snapshot	Sim	Sim	Sim
Política de Autodelete	Não	Não	Não	Política de eficiência
Sim	Sim	Sim	Política de cotas e regra de política de cotas	Sim
Sim	Sim	Fila de recuperação	Sim	Sim
Sim	Volume raiz	Namespace	Sim	Sim
Sim	Dados do utilizador	Não	Não	Não
Qtrees	Não	Não	Não	Quotas
Não	Não	Não	QoS em nível de arquivo	Não

Não	Não	Atributos: estado do volume raiz, garantia de espaço, tamanho, dimensionamento automático e número total de arquivos	Não	Não
Não	QoS de storage	Grupo de políticas de QoS	Sim	Sim
Sim	Fibre Channel (FC)	Não	Não	Não
ISCSI	Não	Não	Não	LUNs
Objeto	Sim	Sim	Sim	grupos
Não	Não	Não	portsets	Não
Não	Não	Números de série	Não	Não
Não	SNMP	v3 utilizadores	Sim	Sim

Limites de storage da recuperação de desastres da SVM

A tabela a seguir mostra o número máximo recomendado de volumes e as relações de recuperação de desastres do SVM com suporte por objeto de storage. Você deve estar ciente de que os limites geralmente dependem da plataforma. Consulte a "Hardware Universe" para saber os limites para a sua configuração específica.

Objeto de storage	Limite
SVM	300 volumes flexíveis
Par de HA	1.000 volumes flexíveis
Cluster	128 relacionamentos de desastre com SVM

Replique configurações da SVM

Fluxo de trabalho de replicação do SnapMirror SVM

A replicação do SnapMirror SVM envolve a criação do SVM de destino, a criação de um cronograma de trabalho de replicação e a criação e inicialização de um relacionamento do SnapMirror.

Você deve determinar qual fluxo de trabalho de replicação mais adequado às suas necessidades:

- "Replique toda uma configuração da SVM"
- "Excluir LIFs e configurações de rede relacionadas da replicação SVM"
- "Exponha a rede, o serviço de nomes e outras configurações da configuração SVM"

Critérios para colocar volumes em SVMs de destino

Ao replicar volumes da SVM de origem para o SVM de destino, é importante saber os critérios de seleção de agregados.

Os agregados são selecionados com base nos seguintes critérios:

- Os volumes são sempre colocados em agregados não-raiz.
- Agregados não-raiz são selecionados com base no espaço livre disponível e no número de volumes já hospedados no agregado.

  Agregados com mais espaço livre e menos volumes têm prioridade. O agregado com a prioridade mais alta é selecionado.

- Volumes de origem em agregados FabricPool são colocados em agregados FabricPool no destino com a mesma política de disposição em camadas.
- Se um volume na SVM de origem estiver localizado em um agregado de Flash Pool, o volume será colocado em um agregado de Flash Pool no SVM de destino, se esse agregado existir e tiver espaço livre suficiente.
- Se a `-space-guarantee` opção do volume replicado estiver definida como `volume`, somente agregados com espaço livre maior que o tamanho do volume serão considerados.
- O tamanho do volume aumenta automaticamente no SVM de destino durante a replicação, com base no tamanho do volume de origem.

  Se você quiser pré-reservar o tamanho no SVM de destino, você deve redimensionar o volume. O tamanho do volume não diminui automaticamente no SVM de destino com base na SVM de origem.

Se você quiser mover um volume de um agregado para outro, use o `volume move` comando na SVM de destino.

Replique toda uma configuração do ONTAP SVM

Você pode criar uma relação de recuperação de desastre do SVM (SVM DR) para replicar uma configuração do SVM para outra. Em caso de desastre no local principal, você pode ativar rapidamente o SVM de destino.

Antes de começar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato. Para obter mais informações, "Crie um relacionamento de pares de cluster"consulte e "Criar um relacionamento entre clusters entre pares".

Para obter a sintaxe completa do comando, consulte a página man.

Sobre esta tarefa

Este fluxo de trabalho pressupõe que você já está usando uma política padrão ou uma política de replicação personalizada.

A partir do ONTAP 9.9,1, quando você usa a política de espelhamento de arquivos, pode criar diferentes políticas de Snapshot na SVM de origem e destino. Além disso, as cópias Snapshot no destino não serão sobrescritas por cópias Snapshot na origem. Para obter mais informações, "Compreensão da replicação do SnapMirror SVM"consulte .

Conclua este procedimento a partir do destino. Se você precisar criar uma nova política de proteção, por exemplo, quando a VM de armazenamento de origem tiver o SMB configurado, crie a política e use a opção **Identity Preserve**. Para obter detalhes, "Crie políticas de proteção de dados personalizadas"consulte .

Passos

Você pode executar esta tarefa a partir do Gerenciador do sistema ou da CLI do ONTAP.

System Manager

1. No cluster de destino, clique em **proteção > relacionamentos**.
2. Em **relacionamentos**, clique em **proteger** e escolha **Storage VMs (DR)**.
3. Selecione uma política de proteção. Se você criou uma política de proteção personalizada, selecione-a e escolha o cluster de origem e a VM de storage que deseja replicar. Você também pode criar uma nova VM de armazenamento de destino inserindo um novo nome de VM de armazenamento.
4. Se desejado, altere as configurações de destino para substituir a preservação de identidade e incluir ou excluir interfaces e protocolos de rede.
5. Clique em **Salvar**.

CLI

1. Criar um SVM de destino:

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   O nome do SVM deve ser exclusivo nos clusters de origem e destino.

   O exemplo a seguir cria um SVM de destino chamado `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

2. No cluster de destino, crie um relacionamento de pares SVM usando o `vserver peer create` comando.

   Para obter mais informações, "Criar um relacionamento entre clusters entre pares"consulte .

3. Criar um agendamento de trabalho de replicação:

   ```
   job schedule cron create -name <job_name> -month <month> -dayofweek
   <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
   ```

   Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

   > O cronograma mínimo com suporte (RPO) para volumes do FlexVol em uma relação do SVM SnapMirror é de 15 minutos. O cronograma mínimo com suporte (RPO) para volumes do FlexGroup em uma relação do SVM SnapMirror é de 30 minutos.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

4. No SVM de destino ou no cluster de destino, crie uma relação de replicação:

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` .

O exemplo a seguir cria uma relação de DR do SnapMirror usando a política padrão `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

O exemplo a seguir cria uma relação de replicação unificada usando a política padrão `MirrorAndVault`:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `async-mirror` , o exemplo a seguir cria uma relação de DR do SnapMirror:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `mirror-vault` , o exemplo a seguir cria uma relação de replicação unificada:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

5. Pare o SVM de destino:

```
vserver stop -vserver <SVM_name>
```

O exemplo a seguir interrompe um SVM de destino chamado SVM_backup:

```
cluster_dst::> vserver stop -vserver svm_backup
```

6. No SVM de destino ou no cluster de destino, inicialize a relação de replicação SVM:

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` .

O exemplo a seguir inicializa a relação entre a SVM de origem e `svm1` o SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Excluir LIFs e configurações de rede relacionadas da replicação SVM

Se as SVMs de origem e destino estiverem em sub-redes diferentes, você poderá usar a `-discard-configs network` opção `snapmirror policy create` do comando para excluir LIFs e configurações de rede relacionadas da replicação SVM.

Antes de começar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

Para obter mais informações, "Crie um relacionamento de pares de cluster"consulte e "Criar um relacionamento entre clusters entre pares".

Sobre esta tarefa

A `-identity-preserve` opção `snapmirror create` do comando deve ser definida como `true` quando você cria a relação de replicação SVM.

Para obter a sintaxe completa do comando, consulte a página man.

Passos

1. Criar um SVM de destino:

`vserver create -vserver SVM -subtype dp-destination`

O nome do SVM deve ser exclusivo nos clusters de origem e destino.

O exemplo a seguir cria um SVM de destino chamado `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. No cluster de destino, crie um relacionamento de pares SVM usando o `vserver peer create` comando.

   Para obter mais informações, "Criar um relacionamento entre clusters entre pares"consulte .

3. Criar uma agenda de trabalhos:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

   > O cronograma mínimo com suporte (RPO) para volumes do FlexVol em uma relação do SVM SnapMirror é de 15 minutos. O cronograma mínimo com suporte (RPO) para volumes do FlexGroup em uma relação do SVM SnapMirror é de 30 minutos.

   O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Criar uma política de replicação personalizada:

   `snapmirror policy create -vserver SVM -policy policy -type async-mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir cria uma política de replicação personalizada para o SnapMirror DR que exclui LIFs:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_exclude_LIFs -type async-mirror -discard-configs network
   ```

   O exemplo a seguir cria uma política de replicação personalizada para replicação unificada que exclui LIFs:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

Considere a criação da mesma política de SnapMirror personalizada no cluster de origem para futuros cenários de failover e failback.

5. No SVM de destino ou no cluster de destino, execute o seguinte comando para criar uma relação de replicação:

   `snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule` *`schedule`* `-policy` *`policy`* `-identity-preserve true|false -discard -configs true|false`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja os exemplos abaixo.

   O exemplo a seguir cria uma relação de DR do SnapMirror que exclui LIFs:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
   -identity-preserve true
   ```

   O exemplo a seguir cria uma relação de replicação unificada da SnapMirror que exclui LIFs:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
   -identity-preserve true -discard-configs true
   ```

6. Pare o SVM de destino:

   `vserver stop`

   `SVM name`

   O exemplo a seguir interrompe o SVM de destino chamado SVM_backup:

   ```
   cluster_dst::> vserver stop -vserver svm_backup
   ```

7. No SVM de destino ou no cluster de destino, inicialize uma relação de replicação:

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir inicializa a relação entre a origem e `svm1` o destino `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Depois de terminar

Você deve configurar a rede e os protocolos no SVM de destino para acesso aos dados em caso de desastre.

Exclua a rede, o serviço de nomes e outras configurações da replicação SVM

Talvez você queira excluir a rede, o serviço de nomes e outras configurações de uma relação de replicação SVM para evitar conflitos ou diferenças de configuração com o SVM de destino.

Você pode usar `-identity-preserve false` a opção `snapmirror create` do comando para replicar apenas os volumes e as configurações de segurança de um SVM. Algumas configurações de protocolo e serviço de nomes também são preservadas.

Sobre esta tarefa

Para obter uma lista das configurações de protocolo e serviço de nomes preservadas, "Configurações replicadas em relacionamentos da SVM DR"consulte .

Para obter a sintaxe completa do comando, consulte a página man.

Antes de começar

Os clusters de origem e destino e as SVMs devem ser colocados em Contato.

Para obter mais informações, "Crie um relacionamento de pares de cluster"consulte e "Criar um relacionamento entre clusters entre pares".

Passos

1. Criar um SVM de destino:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

   O nome do SVM deve ser exclusivo nos clusters de origem e destino.

   O exemplo a seguir cria um SVM de destino chamado `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. No cluster de destino, crie um relacionamento de pares SVM usando o `vserver peer create` comando.

   Para obter mais informações, "Criar um relacionamento entre clusters entre pares"consulte .

3. Criar um agendamento de trabalho de replicação:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

Para `-month`, , `-dayofweek`, e `-hour`, é possível especificar `all` para executar o trabalho todos os meses, dia da semana e hora, respetivamente.

> O cronograma mínimo com suporte (RPO) para volumes do FlexVol em uma relação do SVM SnapMirror é de 15 minutos. O cronograma mínimo com suporte (RPO) para volumes do FlexGroup em uma relação do SVM SnapMirror é de 30 minutos.

O exemplo a seguir cria um horário de trabalho chamado `my_weekly` que é executado aos sábados às 3:00 da manhã:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Crie uma relação de replicação que exclua a rede, o serviço de nomes e outras configurações:

`snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja os exemplos abaixo. Você deve executar esse comando a partir do SVM de destino ou do cluster de destino.

O exemplo a seguir cria uma relação de DR do SnapMirror usando a política padrão `MirrorAllSnapshots`. A relação exclui a rede, o serviço de nomes e outras configurações da replicação SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

O exemplo a seguir cria uma relação de replicação unificada usando a política padrão `MirrorAndVault`. A relação exclui a rede, o serviço de nomes e outras configurações:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `async-mirror` , o exemplo a seguir cria uma relação de DR do SnapMirror. A relação exclui a rede, o serviço de nomes e outras configurações da replicação SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Supondo que você tenha criado uma política personalizada com o tipo de diretiva `mirror-vault` , o exemplo a seguir cria uma relação de replicação unificada. A relação exclui a rede, o serviço de nomes e outras configurações da replicação SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

5. Pare o SVM de destino:

   `vserver stop`

   `SVM name`

   O exemplo a seguir interrompe um SVM de destino chamado dvs1:

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. Se você estiver usando SMB, você também deve configurar um servidor SMB.

   "Somente SMB: Criando um servidor SMB"Consulte .

7. No SVM de destino ou no cluster de destino, inicialize a relação de replicação SVM:

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

Depois de terminar

Você deve configurar a rede e os protocolos no SVM de destino para acesso aos dados em caso de desastre.

Especifique agregados a serem usados para relacionamentos de recuperação de desastres do ONTAP SVM

Após a criação de um SVM para recuperação de desastres, você pode usar a `aggr-list` opção com `vserver modify` comando para limitar quais agregados são usados para hospedar volumes de destino do SVM DR.

Passo

1. Criar um SVM de destino:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. Modifique a lista de agentes do SVM de recuperação de desastres para limitar os agregados usados para hospedar o volume do SVM de recuperação de desastres:

   `cluster_dest::> vserver modify -vserver` *`SVM`* `-aggr-list <comma-separated-list>`

Crie um servidor SMB para um SVM de destino do ONTAP em uma relação de recuperação de desastres

Se o SVM de origem tiver uma configuração SMB e você optar por definir `identity-preserve` como `false`, você deverá criar um servidor SMB para o SVM de destino. O servidor SMB é necessário para algumas configurações SMB, como compartilhamentos durante a inicialização do relacionamento SnapMirror.

Passos

1. Inicie o SVM de destino usando o `vserver start` comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Verifique se o SVM de destino está no `running` estado e se o subtipo está `dp-destination` usando o `vserver show` comando.

```
destination_cluster::> vserver show
                                  Admin      Operational Root
Vserver  Type    Subtype          State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

3. Crie um LIF usando o `network interface create` comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

4. Crie uma rota usando o `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Gerenciamento de rede"

5. Configure o DNS usando o `vserver services dns create` comando.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Adicione o controlador de domínio preferido usando o `vserver cifs domain preferred-dc add` comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Crie o servidor SMB usando o `vserver cifs create` comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Pare o SVM de destino usando o `vserver stop` comando.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Excluir volumes de uma relação de recuperação de desastres do ONTAP SVM

Por padrão, todos os volumes de dados RW da SVM de origem são replicados. Se você não quiser proteger todos os volumes na SVM de origem, use a `-vserver-dr -protection unprotected` opção `volume modify` do comando para excluir volumes da replicação SVM.

Passos

1. Excluir um volume da replicação do SVM:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir exclui o volume `volA_src` da replicação SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

   Se, posteriormente, quiser incluir um volume na replicação SVM que você excluiu originalmente, execute o

seguinte comando:

`volume modify -vserver SVM -volume volume -vserver-dr-protection protected`

O exemplo a seguir inclui o volume `volA_src` na replicação da SVM:

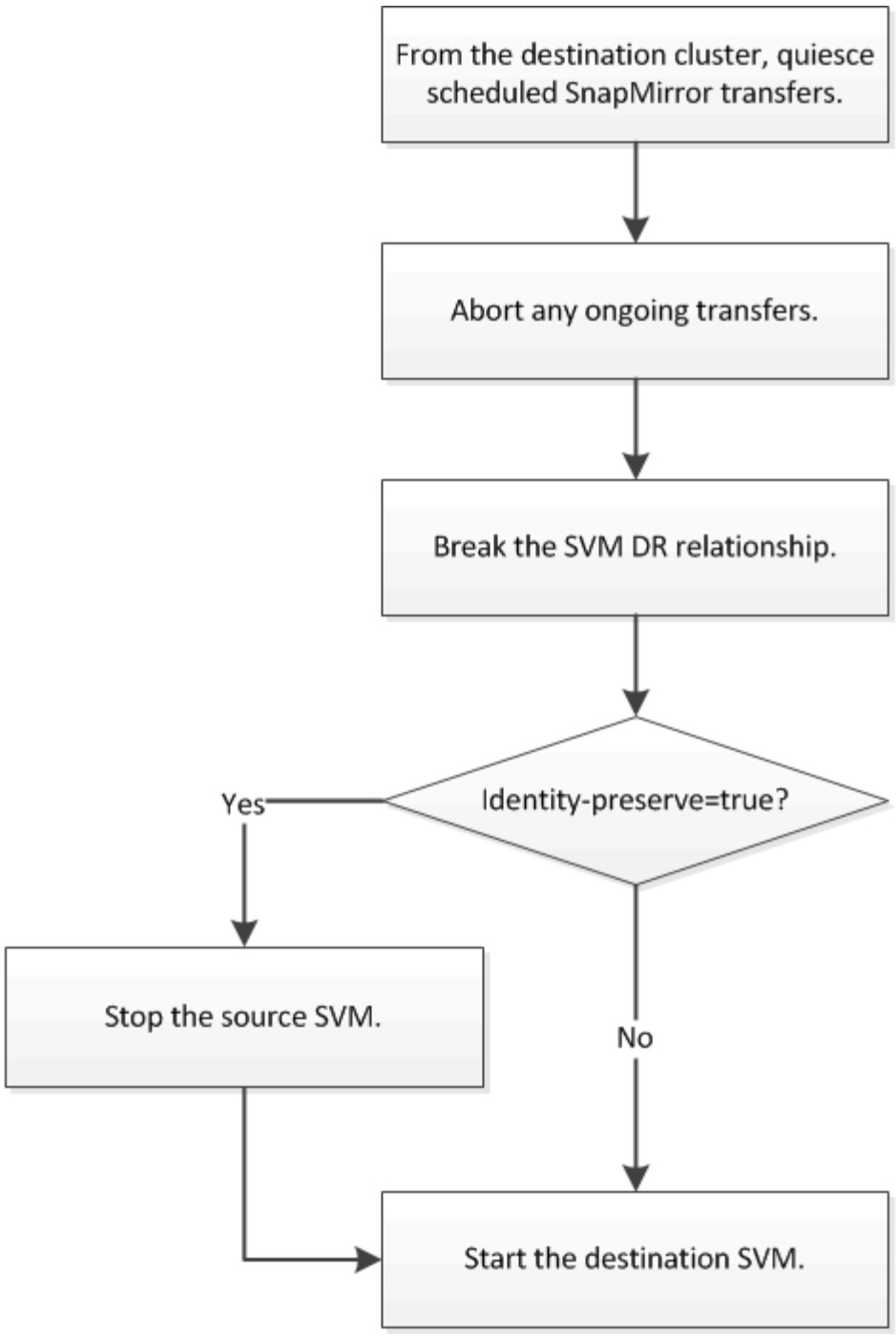
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Crie e inicialize a relação de replicação SVM conforme descrito em "Replicação de toda uma configuração de SVM".

Fornecer dados de um destino com SVM DR

Fluxo de trabalho de recuperação de desastre do ONTAP SVM

Para se recuperar de um desastre e servir dados do SVM de destino, você precisa ativar o SVM de destino. A ativação do SVM de destino envolve a interrupção das transferências agendadas do SnapMirror, o cancelamento das transferências contínuas do SnapMirror, a quebra da relação de replicação, a interrupção da SVM de origem e a inicialização do SVM de destino.



Configurar o volume de destino do ONTAP SVM como gravável

Você precisa fazer com que os volumes de destino do SVM sejam graváveis antes de fornecer dados aos clientes.

O procedimento é em grande parte idêntico ao procedimento para replicação de volume, com uma exceção. Se você definir `-identity-preserve true` quando criou a relação de replicação SVM, será necessário parar o SVM de origem antes de ativar o SVM de destino.

Sobre esta tarefa

Para obter a sintaxe completa do comando, consulte a página man.

Em um cenário de recuperação de desastres, você não pode executar uma atualização do SnapMirror da SVM de origem para o SVM de destino de recuperação de desastres porque sua SVM de origem e seus dados ficarão inacessíveis e porque as atualizações desde o último ressync podem estar ruins ou corrompidas.

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para ativar uma VM de armazenamento de destino após um desastre. A ativação da VM de storage de destino torna os volumes de destino do SVM graváveis e permite que você forneça dados aos clientes.

Passos

Você pode executar esta tarefa a partir do Gerenciador do sistema ou da CLI do ONTAP.

System Manager

1. Se o cluster de origem estiver acessível, verifique se o SVM está parado: Navegue até **Storage > Storage VMs** e verifique a coluna **State** para o SVM.
2. Se o estado da SVM de origem for "em execução", pare-o: Selecione ⋮ e escolha **Stop**.
3. No cluster de destino, localize a relação de proteção desejada: Navegue até **proteção > relacionamentos**.
4. Passe o Mouse sobre o nome da VM de armazenamento de origem desejada, clique ⋮ em e escolha **Ativar destino Storage VM**.
5. Na janela **Ativar VM** de armazenamento de destino, selecione **Ativar a VM de armazenamento de destino e quebre a relação**.
6. Clique em **Ativar**.

CLI

1. No SVM de destino ou no cluster de destino, pare as transferências agendadas para o destino:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

ⓘ Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir interrompe as transferências agendadas entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

2. A partir do SVM de destino ou do cluster de destino, interrompa as transferências contínuas para o destino:

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

ⓘ Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir interrompe as transferências contínuas entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

3. No SVM de destino ou no cluster de destino, interrompa a relação de replicação:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir rompe a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

4. Se você definir `-identity-preserve true` quando criou a relação de replicação SVM, pare o SVM de origem:

```
vserver stop -vserver <SVM>
```

O exemplo a seguir interrompe o SVM de origem `svm1` :

```
cluster_src::> vserver stop svm1
```

5. Inicie o SVM de destino:

```
vserver start -vserver <SVM>
```

O exemplo a seguir inicia o SVM de destino `svm_backup` :

```
cluster_dst::> vserver start svm_backup
```

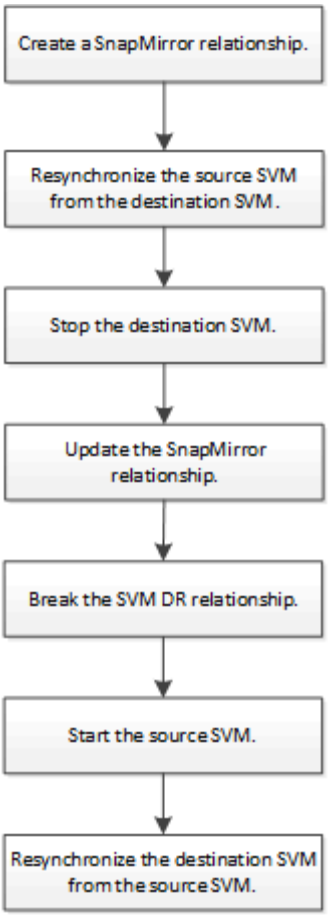
Depois de terminar

Configurar volumes de destino do SVM para acesso aos dados, conforme descrito "Configurar o volume de destino para acesso aos dados"em .

Reative o SVM de origem

Fluxo de trabalho de reativação do SVM de origem ONTAP

Se o SVM de origem existir após um desastre, você poderá reativá-lo e protegê-lo recriando a relação de recuperação de desastres da SVM.



Reative o SVM original da fonte do ONTAP

É possível restabelecer a relação de proteção de dados original entre a fonte e o SVM de destino, quando não precisar mais fornecer dados do destino. O procedimento é em grande parte idêntico ao procedimento para replicação de volume, com uma exceção. É necessário interromper o SVM de destino antes de reativar o SVM de origem.

Antes de começar

Se você tiver aumentado o tamanho do volume de destino ao fornecer dados a partir dele, antes de reativar o volume de origem, você deve aumentar manualmente o dimensionamento máximo no volume de origem original para garantir que ele possa crescer o suficiente.

"Quando um volume de destino cresce automaticamente"

Sobre esta tarefa

A partir do ONTAP 9.11,1, você pode reduzir o tempo de ressincronização durante um ensaio de recuperação de desastres usando a opção CLI do `snapmirror resync` comando enquanto executa uma ressincronização `-quick-resync true`reversa de uma relação SVM DR. Uma ressincronização rápida pode reduzir o tempo necessário para retornar à produção ignorando as operações de reconstrução e restauração do data warehouse.

> A ressincronização rápida não preserva a eficiência de storage dos volumes de destino. A ativação da ressincronização rápida pode aumentar o espaço de volume usado pelos volumes de destino.

Este procedimento pressupõe que a linha de base no volume de origem original está intacta. Se a linha de base não estiver intacta, você deverá criar e inicializar a relação entre o volume do qual você está fornecendo dados e o volume de origem original antes de executar o procedimento.

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para reativar uma VM de armazenamento de origem após um desastre. A reativação da VM de armazenamento de origem interrompe a VM de armazenamento de destino e rehabilita a replicação da origem para o destino.

Quando você usa o System Manager para reativar a VM de armazenamento de origem, o System Manager executa as seguintes operações em segundo plano:

- Cria uma relação de DR SVM reversa do destino original para a fonte original usando o SnapMirror Resync
- Pára o SVM de destino
- Atualiza a relação do SnapMirror
- Quebra o relacionamento SnapMirror
- Reinicia o SVM original
- Emite uma ressincronização SnapMirror da origem original de volta ao destino original
- Limpa as relações SnapMirror

Passos

Você pode executar esta tarefa a partir do Gerenciador do sistema ou da CLI do ONTAP.

System Manager

1. No cluster de destino, clique em **proteção > relacionamentos** e localize a relação de proteção desejada.
2. Passe o Mouse sobre o nome do relacionamento de origem, clique em e selecione **reativar VM de armazenamento de origem**.
3. Na janela **reativar VM** de armazenamento de origem, clique em **reativar**.
4. Em **relacionamentos**, monitore o progresso da reativação da fonte visualizando **Status da transferência** para o relacionamento de proteção. Quando a reativação estiver concluída, o estado do relacionamento deve retornar para "espelhado".

CLI

1. A partir do SVM de origem original ou do cluster de origem original, crie uma relação SVM DR reversa usando a mesma configuração, política e configuração de preservação de identidade que a relação SVM DR original:

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir cria uma relação entre o SVM a partir do qual você está fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

2. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para reverter a relação de proteção de dados:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

> O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. Use `snapmirror initialize` para reinicializar o relacionamento.

O exemplo a seguir inverte a relação entre o SVM de origem original e `svm1` o SVM a partir do qual você está fornecendo dados, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Exemplo usando a opção -Quick-Resync:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. Quando você quiser restabelecer o acesso aos dados à fonte original SVM, pare o SVM de destino original para desconetar todos os clientes conectados ao SVM de destino original.

```
vserver stop -vserver <SVM>
```

O exemplo a seguir interrompe o SVM de destino original que está fornecendo dados no momento:

```
cluster_dst::> vserver stop svm_backup
```

4. Verifique se o SVM de destino original está no estado parado usando o `vserver show` comando.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para executar a atualização final da relação invertida para transferir todas as alterações do SVM de destino original para o SVM de origem original:

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir atualiza a relação entre o SVM de destino original a partir do qual você está fornecendo dados,`svm_backup`e o SVM de origem original `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

6. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para interromper as transferências agendadas para o relacionamento invertido:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir interrompe as transferências agendadas entre o SVM que você está fornecendo dados, `svm_backup` e o SVM original `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. Quando a atualização final estiver concluída e o relacionamento indicar "Quiesced" para o status do relacionamento, execute o seguinte comando da fonte original SVM ou do cluster de origem original para quebrar o relacionamento invertido:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir rompe a relação entre o SVM de destino original do qual você estava fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

8. Se o SVM de origem original tiver sido interrompido anteriormente, a partir do cluster de origem original, inicie o SVM de origem original:

```
vserver start -vserver <SVM>
```

O exemplo a seguir inicia a fonte original SVM:

```
cluster_src::> vserver start svm1
```

9. A partir do SVM de destino original ou do cluster de destino original, restabeleça a relação de proteção de dados original:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir restabelece a relação entre a fonte original SVM e `svm1` o SVM de destino original `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para excluir a relação de proteção de dados invertida:

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir exclui a relação inversa entre o SVM de destino original e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. No SVM de destino original ou no cluster de destino original, solte a relação de proteção de dados invertida:

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir libera a relação inversa entre o SVM de destino original, SVM_backup e a fonte original SVM, `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

Depois de terminar

Use o `snapmirror show` comando para verificar se a relação SnapMirror foi criada. Para obter a sintaxe completa do comando, consulte a página man.

Reative o SVM original de fonte do ONTAP para volumes do FlexGroup

É possível restabelecer a relação de proteção de dados original entre a fonte e o SVM de destino, quando não precisar mais fornecer dados do destino. Para reativar o SVM de origem original quando você estiver usando o FlexGroup volumes, você precisa executar algumas etapas adicionais, incluindo excluir a relação original do SVM DR e liberar a relação original antes de reverter a relação. Você também precisa liberar o relacionamento invertido e recriar o relacionamento original antes de parar as transferências agendadas.

Passos

1. No SVM de destino original ou no cluster de destino original, exclua a relação de DR original do SVM:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir exclui a relação original entre a fonte original SVM, svm1 e o SVM de destino original `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. A partir do SVM de origem original ou do cluster de origem original, solte a relação original e mantenha as cópias Snapshot intactas:

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir libera a relação original entre a fonte original SVM, svm1 e o SVM de destino original, `svm_backup`.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. A partir do SVM de origem original ou do cluster de origem original, crie uma relação SVM DR reversa usando a mesma configuração, política e configuração de preservação de identidade que a relação SVM DR original:

`snapmirror create -source-path SVM: -destination-path SVM:`

> Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir cria uma relação entre o SVM a partir do qual você está fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para reverter a relação de proteção de dados:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

   > O comando falhará se uma cópia Snapshot comum não existir na origem e no destino. Use `snapmirror initialize` para reinicializar o relacionamento.

   O exemplo a seguir inverte a relação entre o SVM de origem original e `svm1` o SVM a partir do qual você está fornecendo dados, `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

5. Quando você quiser restabelecer o acesso aos dados à fonte original SVM, pare o SVM de destino original para desconetar todos os clientes conectados ao SVM de destino original.

   `vserver stop -vserver SVM`

   O exemplo a seguir interrompe o SVM de destino original que está fornecendo dados no momento:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

6. Verifique se o SVM de destino original está no estado parado usando o `vserver show` comando.

```
cluster_dst::> vserver show
                                  Admin      Operational Root
Vserver        Type    Subtype    State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default    stopped    stopped     rv
aggr1
```

7. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para executar a atualização final da relação invertida para transferir todas as alterações do SVM de destino original para o SVM de origem original:

   `snapmirror update -source-path` *SVM*`:` `-destination-path` *SVM*`:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir atualiza a relação entre o SVM de destino original a partir do qual você está fornecendo dados,`svm_backup`e o SVM de origem original `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. No SVM de origem original ou no cluster de origem original, execute o seguinte comando para interromper as transferências agendadas para o relacionamento invertido:

   `snapmirror quiesce -source-path` *SVM*`:` `-destination-path` *SVM*`:`

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir interrompe as transferências agendadas entre o SVM que você está fornecendo dados, `svm_backup` e o SVM original `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

9. Quando a atualização final estiver concluída e o relacionamento indicar "Quiesced" para o status do relacionamento, execute o seguinte comando da fonte original SVM ou do cluster de origem original para quebrar o relacionamento invertido:

   `snapmirror break -source-path` *SVM*`:` `-destination-path` *SVM*`:`

Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

O exemplo a seguir rompe a relação entre o SVM de destino original do qual você estava fornecendo dados e `svm_backup` o SVM de origem original `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

10. Se o SVM de origem original tiver sido interrompido anteriormente, a partir do cluster de origem original, inicie o SVM de origem original:

    `vserver start -vserver` *SVM*

    O exemplo a seguir inicia a fonte original SVM:

    ```
    cluster_src::> vserver start svm1
    ```

11. No SVM de origem original ou no cluster de origem original, exclua a relação SVM DR invertida:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir exclui a relação inversa entre o SVM de destino original, SVM_backup e a fonte original SVM `svm1`:

    ```
    cluster_src::> snapmirror delete -source-path svm_backup: -destination
    -path svm1:
    ```

12. Do SVM de destino original ou do cluster de destino original, libere a relação inversa enquanto mantém as cópias Snapshot intactas:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir libera a relação inversa entre o SVM de destino original, SVM_backup e a fonte original SVM, svm1:

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. A partir do SVM de destino original ou do cluster de destino original, recrie a relação original. Use a mesma configuração, política e configuração de preservação de identidade que a relação original do SVM DR:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir cria uma relação entre a fonte original SVM e `svm1` o SVM de destino original `svm_backup`:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. A partir do SVM de destino original ou do cluster de destino original, restabeleça a relação de proteção de dados original:

    `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

    > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

    O exemplo a seguir restabelece a relação entre a fonte original SVM e `svm1` o SVM de destino original `svm_backup`:

    ```
    cluster_dst::> snapmirror resync -source-path svm1: -destination-path
    svm_backup:
    ```

Ressincronize os dados em um SVM de destino do ONTAP

A partir do ONTAP 9.8, você pode usar o Gerenciador do sistema para ressincronizar os dados e os detalhes de configuração da VM de armazenamento de origem para a VM de armazenamento de destino em um relacionamento de proteção quebrado e restabelecer o relacionamento.

O ONTAP 9.11,1 introduz uma opção para ignorar uma reconstrução completa do data warehouse quando você executa um ensaio de recuperação de desastres, permitindo que você retorne à produção mais rapidamente.

Você executa a operação ressincronizada somente a partir do destino da relação original. A ressincronização exclui todos os dados na VM de armazenamento de destino mais recentes que os dados na VM de

armazenamento de origem.

Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para executar esta tarefa.

System Manager

1. No destino, selecione a relação de proteção desejada: Clique em **proteção > relacionamentos**.
2. Opcionalmente, selecione **execute uma ressincronização rápida** para ignorar uma reconstrução completa do data warehouse durante um ensaio de recuperação de desastres.
3. Clique ⋮ e clique em **Resync**.
4. Em **relacionamentos**, monitore o progresso da ressincronização visualizando **Status da transferência** para o relacionamento.

CLI

1. A partir do cluster de destino, ressincronize a relação:

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

Converter uma relação de recuperação de desastres em volume do ONTAP em uma relação de SVM DR

É possível converter relações de replicação entre volumes para uma relação de replicação entre as máquinas virtuais de armazenamento (SVMs) que possuem os volumes, desde que cada volume na origem (exceto o volume raiz) esteja sendo replicado e cada volume na origem (incluindo o volume raiz) tenha o mesmo nome do volume no destino.

Sobre esta tarefa

Use o `volume rename` comando quando a relação SnapMirror estiver inativa para renomear volumes de destino, se necessário.

Passos

1. No SVM de destino ou no cluster de destino, execute o seguinte comando para ressincronizar os volumes de origem e destino:

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

   > Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

   O exemplo a seguir ressincroniza a relação entre o volume de origem `volA` ligado `svm1` e o volume de destino `volA` ligado `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

2. Crie uma relação de replicação SVM entre as SVMs de origem e destino, conforme descrito em "Replicação de configurações da SVM".

   Você deve usar a `-identity-preserve true` opção `snapmirror create` do comando ao criar sua relação de replicação.

3. Pare o SVM de destino:

   `vserver stop -vserver` *SVM*

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir interrompe o SVM de destino `svm_backup` :

```
cluster_dst::> vserver stop svm_backup
```

4. No SVM de destino ou no cluster de destino, execute o seguinte comando para ressincronizar as SVMs de origem e destino:

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.
   >
   > Embora a ressincronização não exija uma transferência de linha de base, ela pode ser demorada. Você pode querer executar a ressincronização em horas fora do pico.

   O exemplo a seguir ressincroniza a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Exclua uma relação de replicação do ONTAP SVM

Você pode usar os `snapmirror delete` comandos e `snapmirror release` para excluir uma relação de replicação SVM. Em seguida, pode eliminar manualmente volumes de destino desnecessários.

Sobre esta tarefa

`snapmirror release`O comando exclui todas as cópias Snapshot criadas pelo SnapMirror da origem. Você pode usar a `-relationship-info-only` opção para preservar as cópias Snapshot.

Para obter a sintaxe de comando completa nos comandos, consulte a página man.

Passos

1. Execute o seguinte comando a partir do SVM de destino ou do cluster de destino para quebrar a relação de replicação:

   `snapmirror break -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir rompe a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

2. Execute o seguinte comando do SVM de destino ou do cluster de destino para excluir a relação de replicação:

   `snapmirror delete -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir exclui a relação entre o SVM de origem `svm1` e o SVM de destino `svm_backup` :

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

3. Execute o seguinte comando a partir do cluster de origem ou SVM de origem para liberar as informações de relação de replicação da SVM de origem:

   `snapmirror release -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Você deve inserir dois pontos (:) após o nome SVM `-source-path` nas opções e `-destination-path` . Veja o exemplo abaixo.

   O exemplo a seguir libera informações para a relação de replicação especificada da SVM de origem `svm1` :

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

Gerenciar a replicação de volume raiz do SnapMirror

Gerenciar a visão geral da replicação de volume raiz do SnapMirror

Cada SVM em um ambiente nas tem um namespace único. O volume SVM *root,* contendo sistema operacional e informações relacionadas, é o ponto de entrada para a hierarquia do namespace. Para garantir que os dados permaneçam acessíveis aos clientes em caso de interrupção de nó ou failover, crie uma cópia espelhada de compartilhamento de carga do volume raiz do SVM.

O principal objetivo dos espelhos de compartilhamento de carga para volumes raiz do SVM não é mais para compartilhamento de carga; em vez disso, seu objetivo é a recuperação de desastres.

- Se o volume raiz estiver temporariamente indisponível, o espelhamento de compartilhamento de carga fornece automaticamente acesso somente leitura aos dados do volume raiz.
- Se o volume raiz estiver permanentemente indisponível, você poderá promover um dos volumes de compartilhamento de carga para fornecer acesso de gravação aos dados de volume raiz.

Criar e inicializar relações de espelhamento de compartilhamento de carga

Você deve criar um espelhamento de compartilhamento de carga (LSM) para cada volume raiz da SVM que forneça dados nas no cluster. Para clusters que consistam em dois ou mais pares de HA, considere espelhos de compartilhamento de carga dos volumes raiz do SVM para garantir que o namespace permaneça acessível aos clientes caso ambos os nós de um par de HA falhem. Os espelhos de compartilhamento de carga não são adequados para clusters que consistam em um único par de HA.

Sobre esta tarefa

Se você criar um LSM no mesmo nó e o nó não estiver disponível, você terá um único ponto de falha e não terá uma segunda cópia para garantir que os dados permaneçam acessíveis aos clientes. Mas quando você cria o LSM em um nó diferente daquele que contém o volume raiz ou em um par de HA diferente, seus dados ainda estarão acessíveis no caso de uma interrupção.

Por exemplo, em um cluster de quatro nós com um volume raiz em três nós:

- Para o volume raiz no nó 1 do HA 1, crie o LSM no nó HA 2 do HA 1 ou no nó HA 2 do HA 2.
- Para o volume raiz no nó 2 do HA 1, crie o LSM no nó HA 2 do HA 1 ou no nó HA 2 do HA 2.
- Para o volume raiz no nó 1 do HA 2, crie o LSM no nó HA 1 do HA 1 ou no nó HA 1 do HA 2.

Passos

1. Criar um volume de destino para o LSM:

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

O volume de destino deve ser igual ou maior em tamanho do que o volume raiz.

É uma prática recomendada nomear o volume de raiz e destino com sufixos, como `_root` e `_m1`.

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria um volume de espelhamento de compartilhamento de carga para o volume raiz `svm1_root` no `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Crie um cronograma de trabalho de replicações".
3. Crie uma relação de espelhamento de compartilhamento de carga entre o volume raiz da SVM e o volume de destino do LSM:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria uma relação de espelhamento de compartilhamento de carga entre o volume raiz `svm1_root` e o volume de espelhamento de compartilhamento de carga `svm1_m1` :

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

O atributo de tipo do espelho de compartilhamento de carga muda de `DP` para `LS`.

4. Inicialize o espelho de partilha de carga:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir inicializa o espelho de compartilhamento de carga para o volume raiz `svm1_root` :

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

Atualize uma relação de espelhamento de compartilhamento de carga

As relações de espelhamento de compartilhamento de carga (LSM) são atualizadas automaticamente para volumes raiz do SVM depois que um volume no SVM é montado ou desmontado e durante `volume create` operações que incluem a opção "caminho de junção". Você pode atualizar manualmente uma relação LSM se desejar que ela seja atualizada antes da próxima atualização agendada.

As relações de espelhamento de compartilhamento de carga são atualizadas automaticamente nas seguintes circunstâncias:

- É hora de uma atualização agendada
- Uma operação de montagem ou desmontagem é realizada em um volume no volume raiz do SVM
- Um `volume create` comando é emitido que inclui a `juntion-path` opção

Passo

1. Atualize manualmente uma relação de espelhamento de compartilhamento de carga:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   O exemplo a seguir atualiza a relação de espelhamento de compartilhamento de carga para o volume raiz `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

Promova um espelho de compartilhamento de carga

Se um volume raiz estiver permanentemente indisponível, você poderá promover o volume de espelhamento de carga (LSM) para fornecer acesso de gravação aos dados de volume raiz.

O que você vai precisar

Tem de utilizar comandos avançados de nível de privilégio para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Promover um volume LSM:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar

este comando.

```
snapmirror promote -destination-path <SVM:volume>
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir promove o volume `svm1_m2` como o novo volume raiz da SVM:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Introduza `y`. O ONTAP torna o volume LSM um volume de leitura/gravação e exclui o volume raiz original se ele estiver acessível.

> O volume raiz promovido pode não ter todos os dados que estavam no volume raiz original se a última atualização não ocorrer recentemente.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

4. Renomeie o volume promovido seguindo a convenção de nomenclatura usada para o volume raiz:

   Você deve substituir as variáveis entre parênteses angulares pelos valores necessários antes de executar este comando.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   O exemplo a seguir renomeia o volume promovido `svm1_m2` com o nome `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Proteja o volume raiz renomeado, conforme descrito na etapa 3 até a etapa 4 em "Criando e inicializando relações de espelhamento de compartilhamento de carga".

Fazer backup na nuvem

Faça backup dos dados na nuvem usando o SnapMirror

A partir do ONTAP 9.9,1, é possível fazer backup dos dados na nuvem e restaurar os dados do storage de nuvem para um volume diferente usando o Gerenciador do sistema. Você pode usar o StorageGRID ou o ONTAP S3 como armazenamento de objetos na nuvem.

Antes de usar o recurso de nuvem do SnapMirror, você deve solicitar uma chave de licença da API de nuvem do SnapMirror no site de suporte da NetApp: "Solicite a chave de licença da API de nuvem da SnapMirror". Seguindo as instruções, você deve fornecer uma descrição simples da sua oportunidade de negócio e solicitar a chave API enviando um e-mail para o endereço de e-mail fornecido. Você deve receber uma resposta por e-mail dentro de 24 horas com mais instruções sobre como adquirir a chave da API.

Adicionar um armazenamento de objetos na nuvem

Antes de configurar os backups na nuvem do SnapMirror, é necessário adicionar um armazenamento de objetos em nuvem do StorageGRID ou do ONTAP S3.

Passos

1. Clique em **proteção > Visão geral > Cloud Object Stores**.
2. Clique + Add em .

Faça backup usando a política padrão

Você pode configurar rapidamente um backup na nuvem do SnapMirror para um volume existente usando a política de proteção de nuvem padrão, DailyBackup.

Passos

1. Clique em **proteção > Visão geral** e selecione **fazer backup de volumes para o Cloud**.
2. Se esta for a primeira vez que fizer o backup na nuvem, insira sua chave de licença da API da nuvem do SnapMirror no campo de licença, conforme indicado.
3. Clique em **autenticar e continuar**.
4. Selecione um volume de origem.
5. Selecione um armazenamento de objetos na nuvem.
6. Clique em **Salvar**.

Crie uma política de backup personalizada na nuvem

Se você não quiser usar a política de nuvem padrão do DailyBackup para seus backups na nuvem do SnapMirror, você pode criar sua própria política.

Passos

1. Clique em **proteção > Visão geral > Configurações de política local** e selecione **políticas de proteção**.
2. Clique em **Add** e insira os novos detalhes da política.
3. Na seção **tipo de política**, selecione **fazer backup na nuvem** para indicar que você está criando uma política de nuvem.

4. Clique em **Salvar**.

Crie uma cópia de segurança a partir da página volumes

Você pode usar a página System Manager **volumes** quando quiser selecionar e criar backups na nuvem para vários volumes ao mesmo tempo ou quando quiser usar uma política de proteção personalizada.

Passos

1. Clique em **armazenamento > volumes**.
2. Selecione os volumes que deseja fazer backup na nuvem e clique em **proteger**.
3. Na janela **Protect volume**, clique em **More Options** (mais opções).
4. Selecione uma política.

   Você pode selecionar a política padrão, DailyBackup ou uma política de nuvem personalizada criada.

5. Selecione um armazenamento de objetos na nuvem.
6. Clique em **Salvar**.

Restauração a partir da nuvem

Você pode usar o System Manager para restaurar dados de backup do storage de nuvem para um volume diferente no cluster de origem.

> Se você estiver usando o ONTAP 9.16,1 e estiver executando uma restauração de arquivo único na nuvem do SnapMirror para um volume FlexGroup, você só deverá restaurar arquivos para um novo diretório no volume FlexGroup.

Passos

1. No cluster de origem de uma relação SnapMirror-para-nuvem, clique em **armazenamento > volumes**.
2. Selecione o volume que pretende restaurar.
3. Selecione a guia **fazer backup para a nuvem**.
4. Clique ⋮ ao lado do volume de origem que deseja restaurar para exibir o menu e selecione **Restaurar**.
5. Em **fonte**, selecione uma VM de armazenamento e, em seguida, insira o nome do volume para o qual deseja que os dados sejam restaurados.
6. Em **destino**, selecione a cópia Snapshot que deseja restaurar.
7. Clique em **Salvar**.

Excluir uma relação de nuvem do SnapMirror

Você pode usar o System Manager para excluir uma relação de nuvem.

Passos

1. Clique em **armazenamento > volumes** e selecione o volume que deseja excluir.
2. Clique ⋮ ao lado do volume de origem e selecione **Excluir**.
3. Selecione **Excluir o endpoint do armazenamento de objetos na nuvem (opcional)** se você quiser excluir o endpoint do armazenamento de objetos na nuvem.
4. Clique em **Excluir**.

Remover um armazenamento de objetos na nuvem

Você pode usar o System Manager para remover um armazenamento de objetos na nuvem se ele não fizer parte de um relacionamento de backup na nuvem. Quando um armazenamento de objetos em nuvem faz parte de uma relação de backup em nuvem, ele não pode ser excluído.

Passos

1. Clique em **proteção > Visão geral > Cloud Object Stores**.
2. Selecione o armazenamento de objetos que deseja excluir, clique ⋮ e selecione **Excluir**.

Fazer backup dos dados usando o Cloud Backup

A partir do ONTAP 9.9,1, você pode usar o System Manager para fazer backup de dados na nuvem usando o Cloud Backup.

O Cloud Backup é compatível com volumes de leitura-gravação FlexVol e volumes de proteção de dados (DP). A partir do ONTAP 9.12,1, o Cloud Backup dá suporte ao FlexGroup volumes e ao SnapLock volumes.

Antes de começar

Você deve executar os seguintes procedimentos para estabelecer uma conta no BlueXP . Para a conta de serviço, você precisa criar a função como "Administrador da conta". (Outras funções de conta de serviço não têm o Privileges necessário para estabelecer uma conexão do Gerenciador de sistema.)

1. "Crie uma conta no BlueXP ".
2. "Crie um conetor no BlueXP " com um dos seguintes fornecedores de nuvem:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10,1)

   > ⓘ A partir do ONTAP 9.10,1, você pode selecionar o StorageGRID como um fornecedor de backup em nuvem, mas somente se o BlueXP for implantado no local. O BlueXP Connector deve ser instalado no local e disponível por meio do aplicativo software como serviço (SaaS) da BlueXP .

3. "Inscreva-se no Cloud Backup Service em BlueXP " (requer a licença apropriada).
4. "Gere uma chave de acesso e uma chave secreta usando o BlueXP ".

Registre o cluster no BlueXP

Você pode Registrar o cluster no BlueXP usando o BlueXP ou o Gerenciador de sistema.

Passos

1. No System Manager, vá para **Visão geral da proteção**.
2. Sob **Cloud Backup Service**, forneça os seguintes detalhes:
   - ID do cliente
   - Chave secreta do cliente
3. Selecione **Registe-se e continue**.

Habilite o Cloud Backup

Depois que o cluster é registrado no BlueXP , você precisa ativar o backup em nuvem e iniciar o primeiro backup na nuvem.

Passos

1. No Gestor do sistema, clique em **proteção > Visão geral** e, em seguida, desloque-se para a secção **Cloud Backup Service**.
2. Insira **Client ID** e **Client Secret**.

   A partir do ONTAP 9.10,1, você pode aprender sobre o custo de usar a nuvem clicando em **Saiba mais sobre o custo de usar a nuvem**.

3. Clique em **conetar e ativar o Cloud Backup Service**.
4. Na página **Ativar Cloud Backup Service**, forneça os seguintes detalhes, dependendo do fornecedor selecionado.

Para este provedor de nuvem…	Introduza os seguintes dados…
Azure	• ID de subscrição do Azure • Região • Nome do grupo de recursos (existente ou novo)
AWS	• ID da conta da AWS • Chave de acesso • Chave secreta • Região
Projeto Google Cloud (GCP)	• Nome do projeto Google Cloud • Chave de acesso ao Google Cloud • Chave secreta do Google Cloud • Região
StorageGRID (ONTAP 9.10,1 e posterior, e somente para implantação local do BlueXP)	• Servidor • Chave de Acesso SG • Chave secreta SG

5. Selecione uma **Política de proteção**:
   - **Política existente**: Escolha uma política existente.
   - **Nova Política**: Especifique um nome e configure um agendamento de transferência.

     A partir do ONTAP 9.10,1, você pode especificar se deseja ativar o arquivamento com o Azure ou a AWS.

Se você habilitar o arquivamento para um volume com o Azure ou AWS, não será possível desativar o arquivamento.

Se você habilitar o arquivamento para o Azure ou AWS, especifique o seguinte:

- O número de dias após os quais o volume é arquivado.
- O número de cópias de segurança a reter no arquivo. Especifique "0" (zero) para arquivar até o backup mais recente.
- Para AWS, selecione a classe de armazenamento de arquivo.

6. Selecione os volumes que pretende efetuar uma cópia de segurança.
7. Selecione **Guardar**.

Edite a política de proteção usada no Cloud Backup

Você pode alterar a política de proteção usada com o Cloud Backup.

Passos

1. No Gestor do sistema, clique em **proteção > Visão geral** e, em seguida, desloque-se para a secção **Cloud Backup Service**.
2. Clique em e, em seguida, em **Editar**.
3. Selecione uma **Política de proteção**:
   - **Política existente**: Escolha uma política existente.
   - **Nova Política**: Especifique um nome e configure um agendamento de transferência.

A partir do ONTAP 9.10,1, você pode especificar se deseja ativar o arquivamento com o Azure ou a AWS.

Se você habilitar o arquivamento para um volume com o Azure ou AWS, não será possível desativar o arquivamento.

Se você habilitar o arquivamento para o Azure ou AWS, especifique o seguinte:

- O número de dias após os quais o volume é arquivado.
- O número de cópias de segurança a reter no arquivo. Especifique "0" (zero) para arquivar até o backup mais recente.
- Para AWS, selecione a classe de armazenamento de arquivo.

4. Selecione **Guardar**.

Proteger novos volumes ou LUNs na nuvem

Ao criar um novo volume ou LUN, você pode estabelecer uma relação de proteção SnapMirror que permite fazer backup na nuvem para o volume ou LUN.

Antes de começar

- Você deve ter uma licença SnapMirror.
- LIFs entre clusters devem ser configurados.

- NTP deve ser configurado.
- O cluster deve estar executando o ONTAP 9.9,1.

Sobre esta tarefa

Não é possível proteger novos volumes ou LUNs na nuvem nas seguintes configurações de cluster:

- O cluster não pode estar em um ambiente MetroCluster.
- O SVM-DR não é compatível.
- Não é possível fazer backup do FlexGroups usando o Cloud Backup.

Passos

1. Ao provisionar um volume ou LUN, na página **proteção** no Gerenciador de sistema, marque a caixa de seleção **Ativar SnapMirror (local ou remoto)**.
2. Selecione o tipo de política Cloud Backup.
3. Se o backup em nuvem não estiver ativado, selecione **Ativar Cloud Backup Service**.

Proteger volumes ou LUNs existentes na nuvem

É possível estabelecer uma relação de proteção SnapMirror para volumes e LUNs existentes.

Passos

1. Selecione um volume ou LUN existente e clique em **Protect**.
2. Na página **proteger volumes**, especifique **Backup usando o Cloud Backup Service** para a política de proteção.
3. Clique em **Protect**.
4. Na página **proteção**, marque a caixa de seleção **Ativar SnapMirror (local ou remoto)**.
5. Selecione **Ativar Cloud Backup Service**.

Restaurar dados de arquivos de backup

Você pode executar operações de gerenciamento de backup, como restauração de dados, atualização de relacionamentos e exclusão de relacionamentos, somente quando usar a interface do BlueXP . "Restaurar dados de arquivos de backup"Consulte para obter mais informações.

Detalhes técnicos do SnapMirror

Use a correspondência de padrão de nome de caminho

Você pode usar a correspondência de padrões para especificar os caminhos de origem e destino nos `snapmirror` comandos.

```
`snapmirror` os comandos usam nomes de caminho totalmente qualificados no seguinte formato: `vserver:volume`. Você pode abreviar o nome do caminho não inserindo o nome do SVM. Se você fizer isso, o `snapmirror` comando assumirá o contexto local SVM do usuário.
```

Supondo que o SVM seja chamado de "'vserver1'" e o volume seja chamado de "'vol1'", o nome do caminho totalmente qualificado é `vserver1:vol1`.

Você pode usar o asterisco (*) nos caminhos como um curinga para selecionar nomes de caminho correspondentes e totalmente qualificados. A tabela a seguir fornece exemplos de como usar o caractere curinga para selecionar um intervalo de volumes.

`*`	Corresponde a todos os caminhos.
`vs*`	Faz a correspondência de todos os SVMs e volumes com nomes SVM que começam com `vs`.
`:*src`	Corresponde a todos os SVMs com nomes de volume que contêm o `src` texto.
`:vol`	Corresponde a todos os SVMs com nomes de volume começando com `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

Use consultas estendidas para agir em muitos relacionamentos do SnapMirror

Você pode usar *consultas estendidas* para executar operações do SnapMirror em muitos relacionamentos do SnapMirror ao mesmo tempo. Por exemplo, você pode ter várias relações SnapMirror não inicializadas que deseja inicializar usando um comando.

Sobre esta tarefa

Você pode aplicar consultas estendidas às seguintes operações do SnapMirror:

- Inicializando relacionamentos não inicializados
- Retomando relacionamentos quiesced
- Ressincronizar relacionamentos quebrados
- Atualizando relacionamentos ociosos

- A abortar transferências de dados de relacionamento

Passo

1. Execute uma operação SnapMirror em muitos relacionamentos:

   snapmirror command {-state state } *

   O comando a seguir inicializa as relações SnapMirror que estão em um `Uninitialized` estado:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

Garanta uma cópia Snapshot comum em uma implantação de cofre-espelho

Você pode usar o `snapmirror snapshot-owner create` comando para preservar uma cópia Snapshot rotulada no secundário em uma implantação do mirror-Vault. Isso garante que existe uma cópia Snapshot comum para a atualização da relação do Vault.

Sobre esta tarefa

Se você usar uma combinação de fan-out do mirror-Vault ou implantação em cascata, você deve ter em mente que as atualizações falharão se uma cópia Snapshot comum não existir nos volumes de origem e destino.

Esse nunca é um problema para a relação de espelhamento em uma implantação em fan-out ou cascata do mirror-Vault, já que o SnapMirror sempre cria uma cópia Snapshot do volume de origem antes de executar a atualização.

No entanto, pode ser um problema para a relação do Vault, uma vez que o SnapMirror não cria uma cópia Snapshot do volume de origem quando atualiza uma relação do Vault. Você precisa usar o `snapmirror snapshot-owner create` para garantir que haja pelo menos uma cópia Snapshot comum na origem e no destino da relação do Vault.

Passos

1. No volume de origem, atribua um proprietário à cópia Snapshot rotulada que deseja preservar:

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   O exemplo a seguir é designado `ApplicationA` como o proprietário da `snap1` cópia Snapshot:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

2. Atualize a relação do espelho, conforme descrito em "Atualizar manualmente uma relação de replicação".

   Alternativamente, você pode esperar pela atualização agendada do relacionamento espelhado.

3. Transfira a cópia Snapshot rotulada para o destino do Vault:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

`-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot snapshot`

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir transfere a `snap1` cópia Snapshot

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

A cópia Snapshot rotulada será preservada quando a relação do Vault for atualizada.

4. No volume de origem, remova o proprietário da cópia Snapshot rotulada:

`snapmirror snapshot-owner delete -vserver *SVM* -volume *volume* -snapshot *snapshot* -owner *owner*`

Os exemplos a seguir são removidos `ApplicationA` como o proprietário da `snap1` cópia Snapshot:

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

Versões compatíveis do ONTAP para relacionamentos do SnapMirror

Os volumes de origem e destino devem estar executando versões compatíveis do ONTAP antes de criar uma relação de proteção de dados do SnapMirror. Antes de atualizar o ONTAP, você deve verificar se sua versão atual do ONTAP é compatível com a versão de destino do ONTAP para relacionamentos do SnapMirror.

Relacionamentos de replicação unificada

Para relacionamentos SnapMirror do tipo "XDP", usando versões locais ou Cloud Volumes ONTAP:

Começando com ONTAP 9.9,0:

- As versões do ONTAP 9.x,0 são versões somente na nuvem e oferecem suporte a sistemas Cloud Volumes ONTAP. O asterisco (*) após a versão de lançamento indica uma versão somente na nuvem.

> O ONTAP 9.16,0 é uma exceção à regra somente de nuvem fornecendo suporte "Sistemas ASA R2"para o . Os sistemas ASA R2 suportam relações SnapMirror apenas com outros sistemas ASA R2.

- As versões do ONTAP 9.x,1 são versões gerais e oferecem suporte a sistemas locais e Cloud Volumes ONTAP.

> Quando "balanceamento de capacidade avançado" o está ativado em volumes em clusters que executam o ONTAP 9.16.1 ou posterior, as transferências SnapMirror não são compatíveis com clusters que executam versões do ONTAP anteriores ao ONTAP 9.16.1.

A interoperabilidade é bidirecional.

Interoperabilidade para ONTAP versão 9,3 e posterior

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…																				
	9.16.1	9.16.0	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9,9.0*	9,8	9,7	9,6	9,5	9,4	9,3
9.16.1	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.16.0	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.15.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.15.0*	Não	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.14.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não
9.14.0*	Não	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não	Não	Não
9.13.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não
9.13.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	Não	Não	Não	Não
9.12.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não
9.12.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	Não	Não	Não	Não
9.11.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.11.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.10.1	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…																					
9.10.0*	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.9.1	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,9.0*	Não	Não	Não	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,8	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,7	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,6	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	**Sim**
9,5	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
9,4	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	
9,3	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**

Relações síncronas da SnapMirror

O SnapMirror síncrono não é compatível com instâncias de nuvem do ONTAP.

Versão ONTAP…	Interopera com essas versões anteriores do ONTAP…											
	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.16.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não	Não
9.15.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não	Não
9.14.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não
9.13.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.12.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9.11.1	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não	Não
9.10.1	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não	Não

9.9.1	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não	Não
9,8	Não	Não	**Sim**	**Sim**	**Sim**	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**	Não
9,7	Não	Não	Não	**Sim**	**Sim**	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
9,6	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**	**Sim**
9,5	Não	Não	Não	Não	Não	Não	Não	Não	Não	**Sim**	**Sim**	**Sim**

Relações de recuperação de desastres do SnapMirror SVM

Para dados de recuperação de desastres da SVM e proteção contra SVM:

A recuperação de desastres da SVM é compatível apenas entre clusters que executam a mesma versão do ONTAP. **A independência de versão não é suportada para replicação SVM**.

Na recuperação de desastres do SVM para migração SVM:

- A replicação é suportada em uma única direção de uma versão anterior do ONTAP na origem para a mesma ou posterior versão do ONTAP no destino.
- A versão do ONTAP no cluster de destino não deve ser mais do que duas versões principais no local mais recentes ou duas versões principais da nuvem mais recentes, como mostrado na tabela abaixo.
  - A replicação não é compatível com casos de uso de proteção de dados de longo prazo.

O asterisco (*) após a versão de lançamento indica uma versão somente na nuvem.

Para determinar o suporte, localize a versão de origem na coluna da tabela à esquerda e, em seguida, localize a versão de destino na linha superior (DR/migração para versões semelhantes e migração apenas para versões mais recentes).

Fonte	Destino																				
	9,3	9,4	9,5	9,6	9,7	9,8	9,9.0*	9.9.1	9.10.*	9.10.1	9.11.*	9.11.1	9.12.*	9.12.1	9.13.*	9.13.1	9.14.*	9.14.1	9.15.*	9.15.1	9.16.0	9.16.1
9,3	DR/migração	Migração	Migração	Migração	Migração																	
9,4		DR/migração	Migração	Migração	Migração	Migração																
9,5			DR/migração	Migração	Migração	Migração	Migração															
9,6				DR/migração	Migração	Migração	Migração	Migração														

9,7					DR/migração	Migração	Migração	Migração	Migração												
9,8						DR/migração	Migração	Migração	Migração	Migração											
9,9.0*							DR/migração	Migração	Migração	Migração	Migração										
9.9.1								DR/migração	Migração	Migração	Migração	Migração									
9.10.0*									DR/migração	Migração	Migração	Migração	Migração								
9.10.1										DR/migração	Migração	Migração	Migração	Migração							
9.11.0*											DR/migração	Migração	Migração	Migração	Migração						
9.11.1												DR/migração	Migração	Migração	Migração	Migração					
9.12.0*													DR/migração	Migração	Migração	Migração	Migração				
9.12.1														DR/migração	Migração	Migração	Migração	Migração			
9.13.0*															DR/migração	Migração	Migração	Migração	Migração		

9.13.1																DR/migração	Migração	Migração	Migração	Migração	
9.14.0*																	DR/migração	Migração	Migração	Migração	Migração
9.14.1																		DR/migração	Migração	Migração	Migração
9.15.0*																			DR/migração	Migração	Migração
9.15.1																				DR/migração	Migração
9.16.0																					DR/migração
9.16.1																					

Relacionamentos de recuperação de desastres da SnapMirror

Para relações SnapMirror do tipo "DP" e do tipo de política "'assíncrono-mirror'":

Os espelhos do tipo DP não podem ser inicializados a partir do ONTAP 9.11,1 e são completamente obsoletos no ONTAP 9.12,1. Para obter mais informações, "Depreciação de relacionamentos SnapMirror de proteção de dados"consulte .

Na tabela a seguir, a coluna à esquerda indica a versão do ONTAP no volume de origem e a linha superior indica as versões do ONTAP que você pode ter no volume de destino.

Fonte	Destino											
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3	9,2	9,1	9
9.11.1	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.10.1	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não
9.9.1	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não
9,8	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não

9,7	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não	Não
9,6	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
9,5	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não	Não
9,4	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não	Não
9,3	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não	Não
9,2	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não	Não
9,1	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim	Não
9	Não	Não	Não	Não	Não	Não	Não	Não	Não	Sim	Sim	Sim

A interoperabilidade não é bidirecional.

Limitações do SnapMirror

Você deve estar ciente das limitações básicas do SnapMirror antes de criar um relacionamento de proteção de dados.

- Um volume de destino pode ter apenas um volume de origem.

  Um volume de origem pode ter vários volumes de destino. O volume de destino pode ser o volume de origem para qualquer tipo de relação de replicação do SnapMirror.

- Dependendo do modelo do array, você pode distribuir um máximo de oito ou dezesseis volumes de destino a partir de um único volume de origem. Consulte "Hardware Universe"para obter detalhes sobre sua configuração específica.
- Não é possível restaurar arquivos para o destino de uma relação de DR do SnapMirror.
- Os volumes SnapVault de origem ou destino não podem ser de 32 bits.
- O volume de origem de uma relação SnapVault não deve ser um volume FlexClone.

  A relação funcionará, mas a eficiência oferecida pelos volumes FlexClone não será preservada.

Arquivamento e conformidade com a tecnologia SnapLock

O que é SnapLock

O SnapLock é uma solução de conformidade de alto desempenho para organizações que usam storage WORM para reter arquivos de forma não modificada para fins regulatórios e de governança.

O SnapLock ajuda a impedir a exclusão, alteração ou renomeação de dados para atender a regulamentações como SEC 17aa-4(f), HIPAA, FINRA, CFTC e GDPR. Com o SnapLock, você pode criar volumes de propósito especial nos quais arquivos podem ser armazenados e comprometidos com um estado não apagável e não gravável por um período de retenção designado ou indefinidamente. O SnapLock permite que essa retenção seja realizada no nível do arquivo por meio de protocolos padrão de arquivo aberto, como CIFS e NFS. Os

protocolos de arquivos abertos compatíveis com o SnapLock são NFS (versões 2, 3 e 4) e CIFS (SMB 1,0, 2,0 e 3,0).

Com o SnapLock, você envia arquivos e cópias Snapshot para storage WORM e define períodos de retenção para dados protegidos WORM. O storage WORM do SnapLock usa a tecnologia NetApp Snapshot e pode utilizar a replicação SnapMirror e os backups SnapVault como a tecnologia base para fornecer proteção de recuperação de backup para dados. Saiba mais sobre o armazenamento WORM"Armazenamento WORM em conformidade com NetApp SnapLock - TR-4526": .

Você pode usar uma aplicação para comprometer arquivos WORM em NFS ou CIFS, ou usar o recurso de auto-commit do SnapLock para comprometer arquivos para WORM automaticamente. Você pode usar um arquivo anexado *WORM* para reter dados gravados de forma incremental, como informações de log. Para obter mais informações, "Use o modo de adição de volume para criar arquivos anexados WORM"consulte .

O SnapLock é compatível com métodos de proteção de dados que devem atender à maioria dos requisitos de conformidade:

- Você pode usar o SnapLock for SnapVault para proteger cópias Snapshot WORM no storage secundário. "Armazene cópias Snapshot no WORM"Consulte .
- Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres. "Espelhar arquivos WORM"Consulte .

SnapLock é um recurso baseado em licença do NetApp ONTAP. Uma única licença permite que você use o SnapLock em modo de conformidade estrita, para satisfazer mandatos externos, como a regra SEC 17a-4(f), e um modo empresarial mais solto, para atender aos regulamentos internos exigidos para a proteção de ativos digitais. As licenças SnapLock fazem parte do "ONTAP One"pacote de software.

O SnapLock é compatível com todos os sistemas AFF e FAS, bem como com o ONTAP Select. O SnapLock não é uma solução somente de software; é uma solução integrada de hardware e software. Essa distinção é importante para regulamentações WORM rígidas, como a SEC 17a-4(f), que requer uma solução integrada de hardware e software. Para obter mais informações, "SEC Orientação aos corretores-concessionários sobre a utilização de suportes de armazenamento eletrónicos"consulte .

O que você pode fazer com o SnapLock

Depois de configurar o SnapLock, você pode concluir as seguintes tarefas:

- "Armazene dados no WORM"
- "Armazene cópias Snapshot no WORM para storage secundário"
- "Espelhar arquivos WORM para recuperação de desastres"
- "Retenha arquivos WORM durante o litígio usando retenção legal"
- "Exclua arquivos WORM usando o recurso de exclusão privilegiada"
- "Defina o período de retenção do arquivo"
- "Mover um volume SnapLock"
- "Bloqueie uma cópia Snapshot para proteção contra ataques de ransomware"
- "Reveja a utilização do SnapLock com o Registo de Auditoria"
- "Use APIs do SnapLock"

Modos SnapLock Compliance e Enterprise

Os modos SnapLock Compliance e Enterprise diferem principalmente no nível em que cada modo protege arquivos WORM:

Modo SnapLock	Nível de proteção	Exclusão de arquivo WORM durante a retenção
Modo de conformidade	No nível do disco	Não pode ser eliminado
Modo empresarial	No nível do ficheiro	Pode ser excluído pelo administrador de conformidade usando um procedimento auditado de "exclusão privilegiada"

Após o período de retenção ter terminado, você é responsável por excluir quaisquer arquivos que você não precisa mais. Uma vez que um arquivo tenha sido comprometido com WORM, esteja em conformidade ou no modo Enterprise, ele não poderá ser modificado, mesmo depois que o período de retenção expirou.

Não é possível mover um arquivo WORM durante ou após o período de retenção. Você pode copiar um arquivo WORM, mas a cópia não reterá suas características WORM.

A tabela a seguir mostra as diferenças nos recursos suportados pelos modos SnapLock Compliance e Enterprise:

Capacidade	SnapLock Compliance	SnapLock Enterprise
Ative e exclua arquivos usando exclusão privilegiada	Não	Sim
Reinicializar os discos	Não	Sim
Destruir agregados e volumes SnapLock durante o período de retenção	Não	Sim, com exceção do volume de log de auditoria do SnapLock
Renomeie agregados ou volumes	Não	Sim
Use discos que não sejam NetApp	Não	Sim (com "Virtualização FlexArray")
Use o volume SnapLock para o log de auditoria	Sim	Sim, começando com ONTAP 9.5

Recursos suportados e não suportados com o SnapLock

A tabela a seguir mostra os recursos compatíveis com o modo SnapLock Compliance, o modo SnapLock Enterprise ou ambos:

Recurso	Compatível com SnapLock Compliance	Compatível com SnapLock Enterprise
Grupos de consistência	Não	Não
Volumes criptografados	Sim, começando com ONTAP 9.2. Saiba mais Criptografia e SnapLocksobre o .	Sim, começando com ONTAP 9.2. Saiba mais Criptografia e SnapLocksobre o .
FabricPools em agregados SnapLock	Não	Sim, começando com ONTAP 9.8. Saiba mais FabricPool em agregados SnapLock Enterprisesobre o .
Agregados Flash Pool	Sim, começando com ONTAP 9.1.	Sim, começando com ONTAP 9.1.
FlexClone	Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock.	Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock.
Volumes FlexGroup	Sim, começando com ONTAP 9.11,1. Saiba mais [flexgroup]sobre o .	Sim, começando com ONTAP 9.11,1. Saiba mais [flexgroup]sobre o .
LUNs	Não. Saiba mais sobre Suporte LUN o SnapLock.	Não. Saiba mais sobre Suporte LUN o SnapLock.
Configurações do MetroCluster	Sim, começando com ONTAP 9.3. Saiba mais Suporte à MetroClustersobre o .	Sim, começando com ONTAP 9.3. Saiba mais Suporte à MetroClustersobre o .
Verificação multi-admin (MAV)	Sim, começando com ONTAP 9.13,1. Saiba mais Suporte MAVsobre o .	Sim, começando com ONTAP 9.13,1. Saiba mais Suporte MAVsobre o .
SAN	Não	Não
Single-file SnapRestore	Não	Sim
Sincronização ativa do SnapMirror	Não	Não
SnapRestore	Não	Sim
SMTape	Não	Não
SnapMirror síncrono	Não	Não

SSDs	Sim, começando com ONTAP 9.1.	Sim, começando com ONTAP 9.1.
Recursos de eficiência de storage	Sim, começando com ONTAP 9.9,1. Saiba mais suporte à eficiência de storagesobre o .	Sim, começando com ONTAP 9.9,1. Saiba mais suporte à eficiência de storagesobre o .

FabricPool em agregados SnapLock Enterprise

FabricPools são compatíveis com agregados SnapLock Enterprise a partir de ONTAP 9.8. No entanto, sua equipe de conta precisa abrir uma solicitação de variação de produto, documentando que você entende que os dados do FabricPool dispostos em camadas em uma nuvem pública ou privada não são mais protegidos pelo SnapLock porque um administrador da nuvem pode excluir esses dados.

Todos os dados categorizados pelo FabricPool em uma nuvem pública ou privada não são mais protegidos pelo SnapLock porque eles podem ser excluídos por um administrador de nuvem.

Volumes FlexGroup

O SnapLock suporta volumes FlexGroup a partir do ONTAP 9.11,1; no entanto, os seguintes recursos não são suportados:

- Guarda legal
- Retenção baseada em evento
- SnapLock para SnapVault (suportado a partir do ONTAP 9.12,1)

Você também deve estar ciente dos seguintes comportamentos:

- O relógio de conformidade de volume (VCC) de um volume FlexGroup é determinado pelo VCC do componente raiz. Todos os constituintes não-raiz terão seu VCC estreitamente sincronizado com o VCC raiz.
- As propriedades de configuração do SnapLock são definidas apenas no FlexGroup como um todo. Os constituintes individuais não podem ter propriedades de configuração diferentes, como o tempo de retenção padrão e o período de confirmação automática.

Suporte LUN

Os LUNs são compatíveis com volumes SnapLock somente em cenários em que as cópias Snapshot criadas em um volume que não seja SnapLock são transferidas para um volume SnapLock para proteção como parte da relação de cofre do SnapLock. LUNs não são compatíveis com volumes SnapLock de leitura/gravação. No entanto, as cópias Snapshot à prova de violações são compatíveis com volumes de origem e volumes de destino do SnapMirror que contêm LUNs.

Suporte à MetroCluster

O suporte a SnapLock nas configurações do MetroCluster difere entre o modo SnapLock Compliance e o modo SnapLock Enterprise.

SnapLock Compliance

- A partir do ONTAP 9.3, o SnapLock Compliance é compatível com agregados MetroCluster sem espelhamento.

- A partir do ONTAP 9.3, o SnapLock Compliance é compatível com agregados espelhados, mas somente se o agregado for usado para hospedar volumes de log de auditoria do SnapLock.
- As configurações de SnapLock específicas do SVM podem ser replicadas para locais primários e secundários usando o MetroCluster.

SnapLock Enterprise

- A partir do ONTAP 9, os agregados SnapLock Enterprise são compatíveis.
- A partir do ONTAP 9.3, os agregados SnapLock Enterprise com exclusão privilegiada são suportados.
- As configurações de SnapLock específicas da SVM podem ser replicadas para ambos os locais usando o MetroCluster.

Configurações do MetroCluster e relógios de conformidade

As configurações do MetroCluster usam dois mecanismos de relógio de conformidade, o Relógio de conformidade de volume (VCC) e o Relógio de conformidade do sistema (SCC). O VCC e o SCC estão disponíveis para todas as configurações do SnapLock. Quando você cria um novo volume em um nó, seu VCC é inicializado com o valor atual do SCC nesse nó. Depois que o volume é criado, o volume e o tempo de retenção do arquivo são sempre rastreados com o VCC.

Quando um volume é replicado para outro local, seu VCC também é replicado. Quando ocorre uma mudança de volume, do local A ao local B, por exemplo, o VCC continua a ser atualizado no local B, enquanto o SCC no local A pára quando o local A fica offline.

Quando o local A é colocado de volta online e o retorno de volume é executado, o relógio do local A SCC é reiniciado enquanto o VCC do volume continua a ser atualizado. Como o VCC é atualizado continuamente, independentemente das operações de comutação e switchback, os tempos de retenção de arquivos não dependem dos relógios SCC e não se esticam.

Suporte a verificação multi-admin (MAV)

A partir do ONTAP 9.13,1, um administrador de cluster pode ativar explicitamente a verificação de vários administradores em um cluster para exigir aprovação de quorum antes de algumas operações do SnapLock serem executadas. Quando o MAV está ativado, as propriedades de volume do SnapLock, como tempo de retenção padrão, tempo de retenção mínimo, tempo de retenção máximo, modo de adição de volume, período de confirmação automática e exclusão privilegiada, exigirão aprovação de quorum. Saiba mais "MAV"sobre o .

Eficiência de storage

A partir do ONTAP 9.9,1, o SnapLock é compatível com recursos de eficiência de storage, como compactação de dados, deduplicação entre volumes e compressão adaptável para volumes e agregados SnapLock. Para obter mais informações sobre eficiência de storage, "Visão geral da eficiência de storage da ONTAP"consulte .

Criptografia

A ONTAP oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

Isenção de responsabilidade: a NetApp não pode garantir que arquivos WORM protegidos por SnapLock em unidades ou volumes de criptografia automática serão recuperáveis se a chave de autenticação for perdida ou se o número de tentativas de autenticação falhadas exceder o limite especificado e resultar em que a unidade seja permanentemente bloqueada. Você é responsável por garantir contra falhas de autenticação.

A partir do ONTAP 9.2, os volumes criptografados são compatíveis com agregados SnapLock.

Transição de 7 modos

Você pode migrar volumes SnapLock do modo 7 para o ONTAP usando o recurso transição baseada em cópia (CBT) da ferramenta de transição de modo 7D. O modo SnapLock do volume de destino, conformidade ou empresa deve corresponder ao modo SnapLock do volume de origem. Não é possível usar a transição livre de cópias (CFT) para migrar volumes do SnapLock.

Configurar o SnapLock

Configurar o SnapLock

Antes de usar o SnapLock, você precisa configurar o SnapLock executando várias tarefas, "Instale a licença SnapLock"como para cada nó que hospeda um agregado com um volume SnapLock, inicializar o "Relógio de conformidade", criar um agregado SnapLock para clusters que executam versões do ONTAP anteriores ao ONTAP 9.10,1 e "Crie e monte um volume SnapLock"muito mais.

Inicialize o Relógio de conformidade

O SnapLock usa o *volume Compliance Clock* para garantir contra adulteração que pode alterar o período de retenção de arquivos WORM. Você deve primeiro inicializar o *System ComplianceClock* em cada nó que hospeda um agregado SnapLock.

A partir do ONTAP 9.14,1, é possível inicializar ou reinicializar o Relógio de conformidade do sistema quando não houver volumes SnapLock ou nenhum volume com o bloqueio de cópia Snapshot ativado. A capacidade de reinicializar permite que os administradores de sistema redefinam o relógio de conformidade do sistema em casos em que ele pode ter sido inicializado incorretamente ou corrigir a deriva de clock no sistema. No ONTAP 9.13,1 e versões anteriores, depois de inicializar o Relógio de conformidade em um nó, você não poderá iniciá-lo novamente.

Antes de começar

Para reinicializar o Relógio de conformidade:

- Todos os nós no cluster devem estar no estado de integridade.
- Todos os volumes devem estar online.
- Nenhum volume pode estar presente na fila de recuperação.
- Nenhum volume SnapLock pode estar presente.
- Nenhum volume com bloqueio de cópia Snapshot ativado pode estar presente.

Requisitos gerais para inicializar o Relógio de conformidade:

- Você deve ser um administrador de cluster para executar esta tarefa.
- "A licença SnapLock deve ser instalada no nó".

Sobre esta tarefa

O tempo no relógio de conformidade do sistema é herdado pelo *volume Compliance Clock*, o último dos quais controla o período de retenção para arquivos WORM no volume. O volume Compliance Clock é inicializado automaticamente quando você cria um novo volume SnapLock.

A configuração inicial do relógio de conformidade do sistema baseia-se no relógio do sistema de hardware atual. Por esse motivo, você deve verificar se a hora e o fuso horário do sistema estão corretos antes de inicializar o relógio de conformidade do sistema em cada nó. Depois de inicializar o relógio de conformidade do sistema em um nó, você não poderá iniciá-lo novamente quando os volumes SnapLock ou volumes com bloqueio ativado estiverem presentes.

Passos

Você pode usar a CLI do ONTAP para inicializar o Relógio de conformidade ou, a partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para inicializar o Relógio de conformidade.

System Manager

1. Navegue até **Cluster > Overview**.
2. Na seção **nodes**, clique em **Initialize SnapLock Compliance Clock**.
3. Para exibir a coluna **Relógio de conformidade** e verificar se o Relógio de conformidade foi inicializado, na seção **Cluster > Visão geral > nós**, clique em **Mostrar/Ocultar** e selecione **Relógio SnapLock Compliance**.

CLI

1. Inicializar o relógio de conformidade do sistema:

   `snaplock compliance-clock initialize -node` *`node_name`*

   O comando a seguir inicializa o relógio de conformidade do sistema em `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. Quando solicitado, confirme se o relógio do sistema está correto e se deseja inicializar o Relógio de conformidade:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Repita este procedimento para cada nó que hospeda um agregado SnapLock.

Ativar a ressincronização do relógio de conformidade para um sistema configurado por NTP

Pode ativar a funcionalidade de sincronização da hora do Relógio SnapLock Compliance quando um servidor

NTP está configurado.

O que você vai precisar

- Esta funcionalidade está disponível apenas no nível de privilégio avançado.
- Você deve ser um administrador de cluster para executar esta tarefa.
- "A licença SnapLock deve ser instalada no nó".
- Esse recurso está disponível somente para plataformas Cloud Volumes ONTAP, ONTAP Select e VSIM.

Sobre esta tarefa

Quando o daemon de relógio seguro SnapLock deteta uma inclinação além do limite, o ONTAP usa a hora do sistema para redefinir os relógios de conformidade do sistema e do volume. Um período de 24 horas é definido como o limite de inclinação. Isso significa que o relógio de conformidade do sistema é sincronizado com o relógio do sistema somente se o desvio tiver mais de um dia de idade.

O daemon SnapLock secure clock deteta um desvio e altera o Relógio de conformidade para a hora do sistema. Qualquer tentativa de modificar a hora do sistema para forçar o Relógio de conformidade a sincronizar com a hora do sistema falha, uma vez que o Relógio de conformidade sincroniza com a hora do sistema apenas se a hora do sistema for sincronizada com a hora NTP.

Passos

1. Ative o recurso de sincronização da hora do Relógio SnapLock Compliance quando um servidor NTP está configurado:

   `snaplock compliance-clock ntp`

   O comando a seguir habilita o recurso de sincronização da hora do relógio de conformidade do sistema:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. Quando solicitado, confirme se os servidores NTP configurados são confiáveis e se o canal de comunicação é seguro para habilitar o recurso:
3. Verifique se o recurso está ativado:

   `snaplock compliance-clock ntp show`

   O comando a seguir verifica se o recurso de sincronização da hora do relógio de conformidade do sistema está ativado:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Crie um agregado SnapLock

Use a opção volume `-snaplock-type` para especificar um tipo de volume Compliance ou Enterprise SnapLock. Para versões anteriores ao ONTAP 9.10,1, é necessário criar um agregado SnapLock separado. A partir do ONTAP 9.10,1, os volumes SnapLock e

não SnapLock podem existir no mesmo agregado; portanto, você não será mais necessário criar um agregado SnapLock separado se estiver usando o ONTAP 9.10,1.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- O SnapLock "a licença deve ser instalada"no nó. Esta licença está incluída "ONTAP One"no .
- "O Relógio de conformidade no nó tem de ser inicializado".
- Se você tiver particionado os discos como "root", "d.ATA1" e "d.ata2", você deve garantir que os discos sobressalentes estejam disponíveis.

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1, agregados SnapLock e não SnapLock existentes são atualizados para dar suporte à existência de volumes SnapLock e não SnapLock. No entanto, os atributos de volume SnapLock existentes não são atualizados automaticamente. Por exemplo, os campos de compactação de dados, deduplicação entre volumes e deduplicação em segundo plano entre volumes permanecem inalterados. Os novos volumes SnapLock criados com agregados existentes têm os mesmos valores padrão que os volumes que não são SnapLock, e os valores padrão para novos volumes e agregados dependem de plataforma.

Considerações de reversão

Se você precisar reverter para uma versão do ONTAP anterior a 9.10.1, precisará mover todos os volumes SnapLock Compliance, SnapLock Enterprise e SnapLock para seus próprios agregados SnapLock.

Sobre esta tarefa

- Não é possível criar agregados de conformidade para LUNs FlexArray, mas agregados SnapLock Compliance são compatíveis com LUNs FlexArray.
- Não é possível criar agregados de conformidade com a opção SyncMirror.
- Você pode criar agregados de conformidade espelhados em uma configuração do MetroCluster somente se o agregado for usado para hospedar volumes de log de auditoria do SnapLock.

> Em uma configuração MetroCluster, o SnapLock Enterprise é compatível com agregados espelhados e sem espelhamento. O SnapLock Compliance é compatível apenas com agregados sem espelhamento.

Passos

1. Criar um agregado SnapLock:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

A página de manual do comando contém uma lista completa de opções.

O comando a seguir cria um agregado SnapLock `Compliance` nomeado `aggr1` com três discos `node1` no :

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

Criar e montar volumes SnapLock

Você precisa criar um volume SnapLock para os arquivos ou cópias Snapshot que deseja comprometer com o estado WORM. A partir do ONTAP 9.10,1, qualquer volume criado, independentemente do tipo de agregado, é criado por padrão como um volume não SnapLock. Você deve usar a `-snaplock-type` opção para criar explicitamente um volume SnapLock especificando conformidade ou empresa como o tipo SnapLock. Por padrão, o tipo SnapLock está definido como `non-snaplock`.

Antes de começar

- O agregado SnapLock deve estar online.
- Você deve "Verifique se uma licença SnapLock está instalada". Se uma licença do SnapLock não estiver instalada no nó, você deve "instale"fazê-lo. Esta licença está incluída no "ONTAP One". Antes do ONTAP One, a licença SnapLock foi incluída no pacote Segurança e conformidade. O pacote de segurança e conformidade já não é oferecido, mas ainda é válido. Embora não seja necessário atualmente, os clientes existentes podem optar por "Atualize para o ONTAP One".
- "O Relógio de conformidade no nó tem de ser inicializado".

Sobre esta tarefa

Com as permissões de SnapLock adequadas, você pode destruir ou renomear um volume de empresa a qualquer momento. Não é possível destruir um volume de conformidade até que o período de retenção tenha decorrido. Você nunca pode renomear um volume de conformidade.

Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock. O volume do clone será do mesmo tipo de SnapLock que o volume pai.

> LUNs não são compatíveis com volumes SnapLock. Os LUNs são compatíveis com volumes SnapLock somente em cenários em que as cópias Snapshot criadas em um volume que não seja SnapLock são transferidas para um volume SnapLock para proteção como parte da relação de cofre do SnapLock. LUNs não são compatíveis com volumes SnapLock de leitura/gravação. No entanto, as cópias Snapshot à prova de violações são compatíveis com volumes de origem e volumes de destino do SnapMirror que contêm LUNs.

Execute esta tarefa usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

A partir do ONTAP 9.12,1, você pode usar o Gerenciador do sistema para criar um volume SnapLock.

Passos

1. Navegue até **Storage > volumes** e clique em **Add**.
2. Na janela **Adicionar volume**, clique em **mais Opções**.
3. Introduza as novas informações de volume, incluindo o nome e o tamanho do volume.
4. Selecione **Ativar SnapLock** e escolha o tipo SnapLock, Compliance ou Enterprise.
5. Na seção **Auto-commit Files**, selecione **Modified** e insira o tempo que um arquivo deve permanecer inalterado antes que ele seja automaticamente comprometido. O valor mínimo é de 5 minutos e o valor máximo é de 10 anos.
6. Na seção **retenção de dados**, selecione o período de retenção mínimo e máximo.
7. Selecione o período de retenção padrão.
8. Clique em **Salvar**.
9. Selecione o novo volume na página **volumes** para verificar as configurações do SnapLock.

CLI

1. Criar um volume SnapLock:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Para obter uma lista completa de opções, consulte a página de manual do comando. As opções a seguir não estão disponíveis para volumes SnapLock: `-nvfail` `-atime-update` , , `-is -autobalance-eligible` `-space-mgmt-try-first` , E `vmalign`.

O comando a seguir cria um volume SnapLock `Compliance` chamado `vol1` `aggr1` On `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

Monte um volume SnapLock

É possível montar um volume SnapLock em um caminho de junção no namespace SVM para acesso de cliente nas.

O que você vai precisar

O volume SnapLock deve estar online.

Sobre esta tarefa

- É possível montar um volume SnapLock somente sob a raiz do SVM.
- Não é possível montar um volume regular sob um volume SnapLock.

Passos

1. Montar um volume SnapLock:

   `volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir monta um volume SnapLock nomeado `vol1` para o caminho de junção `/sales` no `vs1` namespace:

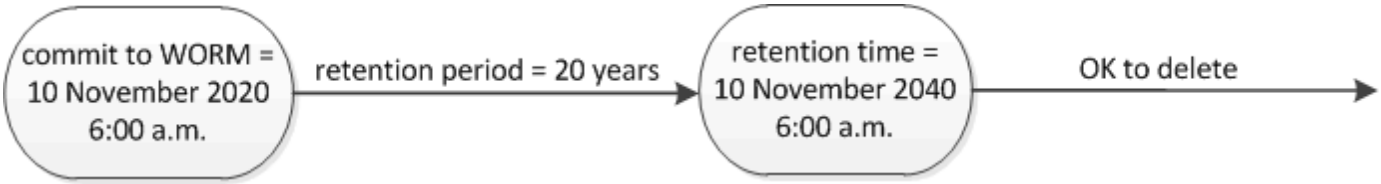
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Defina o tempo de retenção

Você pode definir o tempo de retenção de um arquivo explicitamente ou usar o período de retenção padrão para o volume para obter o tempo de retenção. A menos que você defina o tempo de retenção explicitamente, o SnapLock usará o período de retenção padrão para calcular o tempo de retenção. Você também pode definir a retenção de arquivos após um evento.

Sobre o período de retenção e o tempo de retenção

O *período de retenção* para um arquivo WORM especifica a duração do tempo em que o arquivo deve ser retido depois de ser comprometido com o estado WORM. O *tempo de retenção* para um arquivo WORM é o tempo após o qual o arquivo não precisa mais ser retido. Um período de retenção de 20 anos para um arquivo comprometido com o estado WORM em 10 de novembro de 2020 6:00, por exemplo, permitiria um tempo de retenção de 10 de novembro de 2040 6:00



> A partir do ONTAP 9.10,1, você pode definir um tempo de retenção até 26 de outubro de 3058 e um período de retenção de até 100 anos. Quando você estende as datas de retenção, as políticas mais antigas são convertidas automaticamente. No ONTAP 9.9,1 e versões anteriores, a menos que você defina o período de retenção padrão como infinito, o tempo de retenção máximo suportado é 19 2071 de janeiro (GMT).

Considerações importantes sobre replicação

Ao estabelecer uma relação SnapMirror com um volume de origem SnapLock usando uma data de retenção posterior a 19th 2071 de janeiro (GMT), o cluster de destino deve estar executando o ONTAP 9.10,1 ou posterior ou a transferência SnapMirror falhará.

Considerações importantes de reversão

O ONTAP impede que você reverta um cluster do ONTAP 9.10,1 para uma versão anterior do ONTAP quando houver arquivos com um período de retenção posterior a "19 de janeiro de 2071 8:44:07 AM".

Compreender os períodos de retenção

Um volume SnapLock Compliance ou empresa tem quatro períodos de retenção:

- Período de retenção mínimo (`min`), com um padrão de 0
- Período máximo de retenção (`max`), com um incumprimento de 30 anos
- Período de retenção padrão, com um padrão igual a `min` para o modo de conformidade e o modo Enterprise começando com ONTAP 9.10,1. Nas versões do ONTAP anteriores ao ONTAP 9.10,1, o período de retenção padrão depende do modo:
  - Para o modo de conformidade, o padrão é igual a `max`.
  - Para o modo Enterprise, o padrão é igual a `min`.
- Período de retenção não especificado.

  A partir do ONTAP 9.8, é possível definir o período de retenção de arquivos em um volume como `unspecified`, para permitir que o arquivo seja mantido até que você defina um tempo de retenção absoluto. Você pode definir um arquivo com tempo de retenção absoluto para retenção não especificada e voltar para retenção absoluta, desde que o novo tempo de retenção absoluta seja posterior ao tempo absoluto definido anteriormente.

  A partir do ONTAP 9.12,1, os arquivos WORM com o período de retenção definido como têm a garantia de ter um período de retenção definido `unspecified` para o período de retenção mínimo configurado para o volume SnapLock. Quando você altera o período de retenção de arquivos de `unspecified` para um tempo de retenção absoluto, o novo tempo de retenção especificado deve ser maior do que o tempo de retenção mínimo já definido no arquivo.

Portanto, se você não definir o tempo de retenção explicitamente antes de armazenar um arquivo em modo de conformidade no estado WORM e não modificar os padrões, o arquivo será retido por 30 anos. Da mesma forma, se você não definir o tempo de retenção explicitamente antes de armazenar um arquivo no modo Enterprise no estado WORM e não modificar os padrões, o arquivo será retido por 0 anos ou, efetivamente, não será de todo.

Defina o período de retenção padrão

Você pode usar o `volume snaplock modify` comando para definir o período de retenção padrão para arquivos em um volume SnapLock.

O que você vai precisar

O volume SnapLock deve estar online.

Sobre esta tarefa

A tabela a seguir mostra os valores possíveis para a opção período de retenção padrão:

> O período de retenção predefinido deve ser superior ou igual a (>) o período de retenção mínimo e inferior ou igual a (>) o período de retenção máximo.

Valor	Unidade	Notas
0 - 65535	segundos	
0 - 24	horas	

Valor	Unidade	Notas
0 - 365	dias	
0 - 12	meses	
0 - 100	anos	Começando com ONTAP 9.10,1. Para versões anteriores do ONTAP, o valor é 0 - 70.
máx	-	Use o período de retenção máximo.
mín	-	Use o período de retenção mínimo.
infinito	-	Guarde os arquivos para sempre.
não especificado	-	Guarde os arquivos até que um período de retenção absoluto seja definido.

Os valores e intervalos para os períodos de retenção máximo e mínimo são idênticos, exceto para `max` e `min`, que não são aplicáveis. Para obter mais informações sobre esta tarefa, "Defina a visão geral do tempo de retenção"consulte .

Você pode usar o `volume snaplock show` comando para exibir as configurações do período de retenção do volume. Para obter mais informações, consulte a página man para o comando.

Depois que um arquivo foi comprometido com o estado WORM, você pode estender, mas não reduzir o período de retenção.

Passos

1. Defina o período de retenção padrão para arquivos em um volume SnapLock:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-default -retention-period` *`default_retention_period`* `-minimum-retention-period` *`min_retention_period`* `-maximum-retention-period` *`max_retention_period`*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   Os exemplos a seguir pressupõem que os períodos de retenção mínimo e máximo não foram modificados anteriormente.

   O comando a seguir define o período de retenção padrão para um volume de conformidade ou empresa para 20 dias:

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

O comando a seguir define o período de retenção padrão para um volume de conformidade para 70 anos:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

O comando a seguir define o período de retenção padrão para um volume Enterprise para 10 anos:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Os comandos a seguir definem o período de retenção padrão para um volume Enterprise para 10 dias:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

O comando a seguir define o período de retenção padrão para um volume de conformidade como infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Defina o tempo de retenção de um arquivo explicitamente

Você pode definir o tempo de retenção de um arquivo explicitamente modificando seu último tempo de acesso. Você pode usar qualquer comando ou programa adequado em NFS ou CIFS para modificar o último tempo de acesso.

Sobre esta tarefa

Depois que um arquivo foi comprometido com WORM, você pode estender, mas não reduzir o tempo de retenção. O tempo de retenção é armazenado `atime` no campo para o arquivo.

> Não é possível definir explicitamente o tempo de retenção de um arquivo como `infinite`. Esse valor só está disponível quando você usa o período de retenção padrão para calcular o tempo de retenção.

Passos

1. Use um comando ou programa adequado para modificar a última hora de acesso para o arquivo cujo tempo de retenção você deseja definir.

   Em um shell UNIX, use o seguinte comando para definir um tempo de retenção de 21 de novembro de 2020 6:00 em um arquivo chamado `document.txt`:

```
touch -a -t 202011210600 document.txt
```

Você pode usar qualquer comando ou programa adequado para modificar a última hora de acesso no Windows.

Defina o período de retenção do arquivo após um evento

A partir do ONTAP 9.3, você pode definir quanto tempo um arquivo é retido após um evento ocorrer usando o recurso SnapLock *retenção baseada em eventos (EBR)*.

O que você vai precisar

- Você deve ser um administrador do SnapLock para executar esta tarefa.

  "Crie uma conta de administrador do SnapLock"

- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Sobre esta tarefa

A política de retenção *evento* define o período de retenção para o arquivo após o evento ocorrer. A política pode ser aplicada a um único arquivo ou a todos os arquivos em um diretório.

- Se um arquivo não for um arquivo WORM, ele será comprometido com o estado WORM durante o período de retenção definido na política.
- Se um arquivo for um arquivo WORM ou um arquivo anexado WORM, seu período de retenção será estendido pelo período de retenção definido na política.

Você pode usar um volume de modo de conformidade ou de modo empresarial.

As políticas EBR não podem ser aplicadas a ficheiros sob retenção legal.

Para uma utilização avançada, "Storage WORM em conformidade com NetApp SnapLock"consulte .

usando EBR para estender o período de retenção de arquivos WORM já existentes
O EBR é conveniente quando você deseja estender o período de retenção de arquivos WORM já existentes. Por exemplo, pode ser política da sua empresa manter os Registros W-4 de funcionários em forma não modificada por três anos após o funcionário mudar uma eleição de retenção. Outra política da empresa pode exigir que os Registros W-4 sejam mantidos por cinco anos após o término do funcionário. Nessa situação, você pode criar uma política de EBR com um período de retenção de cinco anos. Depois que o funcionário for rescindido (o "evento"), você aplicará a política EBR ao Registro W-4 do funcionário, fazendo com que seu período de retenção seja estendido. Isso geralmente será mais fácil do que estender o período de retenção manualmente, especialmente quando um grande número de arquivos está envolvido.

Passos

1. Criar uma política EBR:

   ```
   snaplock event-retention policy create -vserver SVM_name -name policy_name
   -retention-period retention_period
   ```

O comando a seguir cria a política de EBR `employee_exit vs1` com um período de retenção de dez anos:

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name
employee_exit -retention-period 10years
```

2. Aplicar uma política EBR:

snaplock event-retention apply -vserver *SVM_name* -name *policy_name* -volume *volume_name* -path *path_name*

O comando a seguir aplica a diretiva EBR `employee_exit vs1` a todos os arquivos no diretório `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name
employee_exit -volume vol1 -path /d1
```

Criar um log de auditoria

Se você estiver usando o ONTAP 9.9,1 ou anterior, primeiro você deve criar um agregado SnapLock e, em seguida, criar um log de auditoria protegido por SnapLock antes de executar uma exclusão privilegiada ou movimentação de volume SnapLock. O log de auditoria Registra a criação e exclusão de contas de administrador do SnapLock, modificações no volume de log, se a exclusão privilegiada está ativada, operações de exclusão privilegiada e operações de movimentação de volume do SnapLock.

A partir do ONTAP 9.10,1, você não cria mais um agregado SnapLock. Você deve usar a opção -SnapLock -type para "Crie explicitamente um volume SnapLock"especificando conformidade ou empresa como o tipo SnapLock.

Antes de começar

Se você estiver usando o ONTAP 9.9,1 ou anterior, será necessário ser um administrador de cluster para criar um agregado SnapLock.

Sobre esta tarefa

Não é possível excluir um log de auditoria até que o período de retenção do arquivo de log tenha decorrido. Não é possível modificar um registo de auditoria mesmo depois de decorrido o período de retenção. Isso é verdade para os modos SnapLock Compliance e Enterprise.

> No ONTAP 9.4 e anteriores, não é possível usar um volume SnapLock Enterprise para o log de auditoria. Você deve usar um volume SnapLock Compliance. No ONTAP 9.5 e posterior, você pode usar um volume SnapLock Enterprise ou um volume SnapLock Compliance para o log de auditoria. Em todos os casos, o volume do log de auditoria deve ser montado no caminho de `/snaplock_audit_log` junção . Nenhum outro volume pode usar este caminho de junção.

Você pode encontrar os logs de auditoria do SnapLock `/snaplock_log` no diretório sob a raiz do volume de log de auditoria, em subdiretórios `privdel_log` nomeados (operações de exclusão privilegiadas) e `system_log` (tudo o resto). Os nomes dos arquivos de log de auditoria contêm o carimbo de data/hora da

primeira operação registrada, facilitando a pesquisa de Registros pelo tempo aproximado em que as operações foram executadas.

- Você pode usar o `snaplock log file show` comando para exibir os arquivos de log no volume de log de auditoria.
- Você pode usar o `snaplock log file archive` comando para arquivar o arquivo de log atual e criar um novo, o que é útil nos casos em que você precisa Registrar informações de log de auditoria em um arquivo separado.

Para obter mais informações, consulte as páginas man para os comandos.

Um volume de proteção de dados não pode ser usado como um volume de log de auditoria do SnapLock.

Passos

1. Crie um agregado SnapLock.

   Crie um agregado SnapLock

2. No SVM que você deseja configurar para o log de auditoria, crie um volume SnapLock.

   Crie um volume SnapLock

3. Configure o SVM para o log de auditoria:

   `snaplock log create -vserver` *`SVM_name`* `-volume` *`snaplock_volume_name`* `-max-log -size` *`size`* `-retention-period` *`default_retention_period`*

   O período de retenção padrão mínimo para arquivos de log de auditoria é de seis meses. Se o período de retenção de um arquivo afetado for maior do que o período de retenção do log de auditoria, o período de retenção do log herdará o período de retenção do arquivo. Assim, se o período de retenção para um arquivo excluído usando exclusão privilegiada for de 10 meses, e o período de retenção do log de auditoria for de 8 meses, o período de retenção do log será estendido para 10 meses. Para obter mais informações sobre o tempo de retenção e o período de retenção padrão, "Defina o tempo de retenção"consulte .

   O comando a seguir configura-se `SVM1` para o log de auditoria usando o volume SnapLock `logVol` . O log de auditoria tem um tamanho máximo de 20 GB e é mantido por oito meses.

   ```
   SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
   20GB -retention-period 8months
   ```

4. No SVM que você configurou para o log de auditoria, monte o volume SnapLock no caminho de `/snaplock_audit_log` junção .

   Monte um volume SnapLock

Verifique as configurações do SnapLock

Use os `volume file fingerprint start` comandos e `volume file`

`fingerprint dump` para visualizar as principais informações sobre arquivos e volumes, incluindo o tipo de arquivo (normal, WORM ou WORM anexado), a data de expiração do volume e assim por diante.

Passos

1. Gerar uma impressão digital de arquivo:

   `volume file fingerprint start -vserver <SVM_name> -file <file_path>`

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   O comando gera um Session ID que você pode usar como entrada para o `volume file fingerprint dump` comando.

   > Você pode usar o `volume file fingerprint show` comando com o Session ID para monitorar o andamento da operação de impressão digital. Certifique-se de que a operação foi concluída antes de tentar exibir a impressão digital.

2. Exibir a impressão digital do arquivo:

   `volume file fingerprint dump -session-id <session_ID>`

   ```
   svm1::> volume file fingerprint dump -session-id 33619976
           Vserver:svm1
           Session-ID:33619976
           Volume:slc_vol
           Path:/vol/slc_vol/f1
           Data
   Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

   Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
   Algorithm:SHA256
           Fingerprint Scope:data-and-metadata
           Fingerprint Start Time:1460612586
           Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
           Fingerprint Version:3
           **SnapLock License:available**
           Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
           Volume MSID:2152884007
           Volume DSID:1028
           Hostname:my_host
           Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
           Volume Containing Aggregate:slc_aggr1
   ```

```
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Gerenciar arquivos WORM

Gerenciar arquivos WORM

Você pode gerenciar arquivos WORM das seguintes maneiras:

- "Armazene dados no WORM"
- "Armazene cópias Snapshot em WORM em um destino de cofre"
- "Espelhar arquivos WORM para recuperação de desastres"
- "Retenha arquivos WORM durante o litígio"
- "Exclua arquivos WORM"

Armazene dados no WORM

Você pode comprometer arquivos para WORM (uma gravação, muitas leituras) manualmente ou armazená-los automaticamente. Você também pode criar arquivos anexados WORM.

Armazene dados em WORM manualmente

Armazene um arquivo no WORM manualmente, fazendo o arquivo somente leitura. Você pode usar qualquer comando ou programa adequado sobre NFS ou CIFS para alterar o atributo de leitura e gravação de um arquivo para somente leitura. Você pode optar por enviar arquivos manualmente se quiser garantir que um aplicativo tenha terminado de gravar em um arquivo para que o arquivo não seja comprometido prematuramente ou se houver problemas de dimensionamento para o scanner de confirmação automática por causa de um grande número de volumes.

O que você vai precisar

- O arquivo que você deseja confirmar deve residir em um volume SnapLock.
- O ficheiro tem de ser gravável.

Sobre esta tarefa

O volume ComplianceClock Time é gravado `ctime` no campo do arquivo quando o comando ou programa é executado. A hora do ComplianceClock determina quando o tempo de retenção para o arquivo foi atingido.

Passos

1. Use um comando ou programa adequado para alterar o atributo de leitura e gravação de um arquivo para somente leitura.

   Em um shell UNIX, use o seguinte comando para criar um arquivo chamado `document.txt` somente leitura:

   ```
   chmod -w document.txt
   ```

   Em um shell do Windows, use o seguinte comando para criar um arquivo chamado `document.txt` somente leitura:

   ```
   attrib +r document.txt
   ```

Armazene dados no WORM automaticamente

O recurso de autocommit do SnapLock permite que você armazene arquivos no WORM automaticamente. O recurso de confirmação automática vincula um arquivo ao estado WORM em um volume SnapLock se o arquivo não for alterado durante o período de confirmação automática. O recurso de confirmação automática está desativado por padrão.

O que você vai precisar

- Os arquivos que você deseja confirmar automaticamente devem residir em um volume SnapLock.
- O volume SnapLock deve estar online.
- O volume SnapLock deve ser um volume de leitura e gravação.

O recurso de confirmação automática do SnapLock verifica todos os arquivos no volume e envia um arquivo se ele atender ao requisito de confirmação automática. Pode haver um intervalo de tempo entre quando o arquivo está pronto para o autocommit e quando ele é realmente confirmado pelo scanner de autocommit SnapLock. No entanto, o arquivo ainda está protegido de modificações e exclusão pelo sistema de arquivos assim que for elegível para autocommit.

Sobre esta tarefa

O *autocommit period* especifica o período de tempo em que os arquivos devem permanecer inalterados antes de serem autocommitidos. A alteração de um arquivo antes do término do período de confirmação automática reinicia o período de confirmação automática do arquivo.

A tabela a seguir mostra os valores possíveis para o período de confirmação automática:

Valor	Unidade	Notas
nenhum	-	O padrão.
5 - 5256000	minutos	-
1 - 87600	horas	-
1 - 3650	dias	-
1 - 120	meses	-
1 - 10	anos	-

O valor mínimo é de 5 minutos e o valor máximo é de 10 anos.

Passos

1. Arquivos AUTOCOMMIT em um volume SnapLock para WORM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-autocommit -period` *`autocommit_period`*

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir autocommits os arquivos no `vol1` volume do SVM VS1, desde que os arquivos permaneçam inalterados por 5 horas:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

Crie um arquivo anexado WORM

Um arquivo anexado WORM retém os dados gravados de forma incremental, como entradas de log. Você pode usar qualquer comando ou programa adequado para criar um arquivo anexado WORM ou usar o

recurso SnapLock *volume append mode* para criar arquivos anexados WORM por padrão.

Use um comando ou programa para criar um arquivo anexado WORM

Você pode usar qualquer comando ou programa adequado em NFS ou CIFS para criar um arquivo anexado WORM. Um arquivo anexado WORM retém os dados gravados de forma incremental, como entradas de log. Os dados são anexados ao arquivo em blocos de 256 KB. À medida que cada pedaço é escrito, o pedaço anterior se torna protegido WORM. Não é possível eliminar o ficheiro até que o período de retenção tenha decorrido.

O que você vai precisar

O arquivo WORM anexado deve residir em um volume SnapLock.

Sobre esta tarefa

Os dados não precisam ser gravados sequencialmente no bloco ativo de 256 KB. Quando os dados são gravados no byte n 256KB e 1 do arquivo, o segmento anterior de 256 KB fica protegido por WORM.

Qualquer gravação não ordenada além do bloco ativo de 256 KB atual resultará na redefinição do bloco ativo de 256KB para o último deslocamento e fará com que as gravações em desvios mais antigos falhem com um erro 'Read Only File System (ROFS)'. Os desvios de gravação dependem do aplicativo cliente. Um cliente que não esteja em conformidade com a semântica de gravação de arquivo WORM append pode causar o encerramento incorreto do conteúdo de gravação. Portanto, é recomendável garantir que o cliente siga as restrições de deslocamento para gravações não ordenadas ou garantir gravações síncronas montando o sistema de arquivos no modo síncrono.

Passos

1. Use um comando ou programa adequado para criar um arquivo de comprimento zero com o tempo de retenção desejado.

   Em um shell UNIX, use o seguinte comando para definir um tempo de retenção de 21 de novembro de 2020 6:00 em um arquivo de comprimento zero chamado `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Use um comando ou programa adequado para alterar o atributo de leitura e gravação do arquivo para somente leitura.

   Em um shell UNIX, use o seguinte comando para criar um arquivo chamado `document.txt` somente leitura:

   ```
   chmod 444 document.txt
   ```

3. Use um comando ou programa adequado para alterar o atributo de leitura e gravação do arquivo de volta para gravável.

   Esta etapa não é considerada um risco de conformidade porque não há dados no arquivo.

   Em um shell UNIX, use o seguinte comando para fazer um arquivo chamado `document.txt` gravável:

```
chmod 777 document.txt
```

4. Use um comando ou programa adequado para começar a gravar dados no arquivo.

   Em um shell UNIX, use o seguinte comando para gravar dados no `document.txt`:

```
echo test data >> document.txt
```

> Altere as permissões de arquivo de volta para somente leitura quando você não precisar mais anexar dados ao arquivo.

Use o modo de adição de volume para criar arquivos anexados WORM

A partir do ONTAP 9.3, você pode usar o recurso SnapLock *volume append mode* (VAM) para criar arquivos anexados WORM por padrão. Um arquivo anexado WORM retém os dados gravados de forma incremental, como entradas de log. Os dados são anexados ao arquivo em blocos de 256 KB. À medida que cada pedaço é escrito, o pedaço anterior se torna protegido WORM. Não é possível eliminar o ficheiro até que o período de retenção tenha decorrido.

O que você vai precisar

- O arquivo WORM anexado deve residir em um volume SnapLock.
- O volume SnapLock deve estar desmontado e vazio de cópias Snapshot e arquivos criados pelo usuário.

Sobre esta tarefa

Os dados não precisam ser gravados sequencialmente no bloco ativo de 256 KB. Quando os dados são gravados no byte n 256KB e 1 do arquivo, o segmento anterior de 256 KB fica protegido por WORM.

Se você especificar um período de auto-commit para o volume, os arquivos anexados WORM que não são modificados por um período maior do que o período de auto-commit são comprometidos com WORM.

> O VAM não é compatível com volumes de log de auditoria do SnapLock.

Passos

1. Ativar VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Para obter uma lista completa de opções, consulte a página de manual do comando.

   O comando a seguir habilita o VAM no `vol1` volume de SVM`vs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. Use um comando ou programa adequado para criar arquivos com permissões de gravação.

Por padrão, os arquivos são anexados WORM.

Armazene snapshots em WORM em um destino de cofre

Você pode usar o SnapLock for SnapVault para proteger snapshots WORM no storage secundário. Você executa todas as tarefas básicas do SnapLock no destino do Vault. O volume de destino é montado automaticamente somente leitura, portanto, não é necessário comprometer explicitamente os snapshots para WORM.

Antes de começar

- Se você quiser usar o Gerenciador do sistema para configurar o relacionamento, os clusters de origem e destino devem estar executando o ONTAP 9.15,1 ou posterior.
- No cluster de destino:
  - "Instale a licença SnapLock".
  - "Inicialize o Relógio de conformidade".
  - Se você estiver usando a CLI com uma versão do ONTAP anterior a 9.10.1, "Crie um agregado SnapLock".
- A política de proteção deve ser do tipo "Vault".
- Os agregados de origem e destino devem ser de 64 bits.
- O volume de origem não pode ser um volume SnapLock.
- Se você estiver usando a CLI do ONTAP, os volumes de origem e destino devem ser criados no "clusters com peered" e "SVMs"no .

Sobre esta tarefa

O volume de origem pode usar armazenamento NetApp ou não NetApp. Para armazenamento que não seja NetApp, você deve usar a virtualização FlexArray.

Não é possível renomear um snapshot com compromisso com o estado WORM.

Você pode clonar volumes do SnapLock, mas não pode clonar arquivos em um volume do SnapLock.

LUNs não são compatíveis com volumes SnapLock. Os LUNs são compatíveis com volumes SnapLock somente em cenários em que os snapshots criados em um volume que não seja SnapLock são transferidos para um volume SnapLock para proteção como parte da relação de cofre do SnapLock. LUNs não são compatíveis com volumes SnapLock de leitura/gravação. No entanto, snapshots à prova de violações são compatíveis com volumes de origem do SnapMirror e volumes de destino que contêm LUNs.

A partir do ONTAP 9.10,1, os volumes SnapLock e não SnapLock podem existir no mesmo agregado; portanto, você não será mais necessário criar um agregado SnapLock separado se estiver usando o ONTAP 9.10,1. Você usa a opção volume '-SnapLock-type' para especificar um tipo de volume Compliance ou Enterprise SnapLock. Nas versões do ONTAP anteriores ao ONTAP 9.10,1, o modo SnapLock, Compliance ou Enterprise é herdado do agregado. Os volumes de destino flexíveis de versão não são suportados. A definição de idioma do volume de destino tem de corresponder à definição de idioma do volume de origem.

Um volume SnapLock que é um destino do Vault tem um período de retenção padrão atribuído a ele. O valor para este período é inicialmente definido para um mínimo de 0 anos para volumes SnapLock Enterprise e um máximo de 30 anos para volumes SnapLock Compliance. Primeiro, cada snapshot do NetApp é comprometido

com esse período de retenção padrão. O período de retenção pode ser estendido mais tarde, se necessário. Para obter mais informações, "Defina a visão geral do tempo de retenção"consulte .

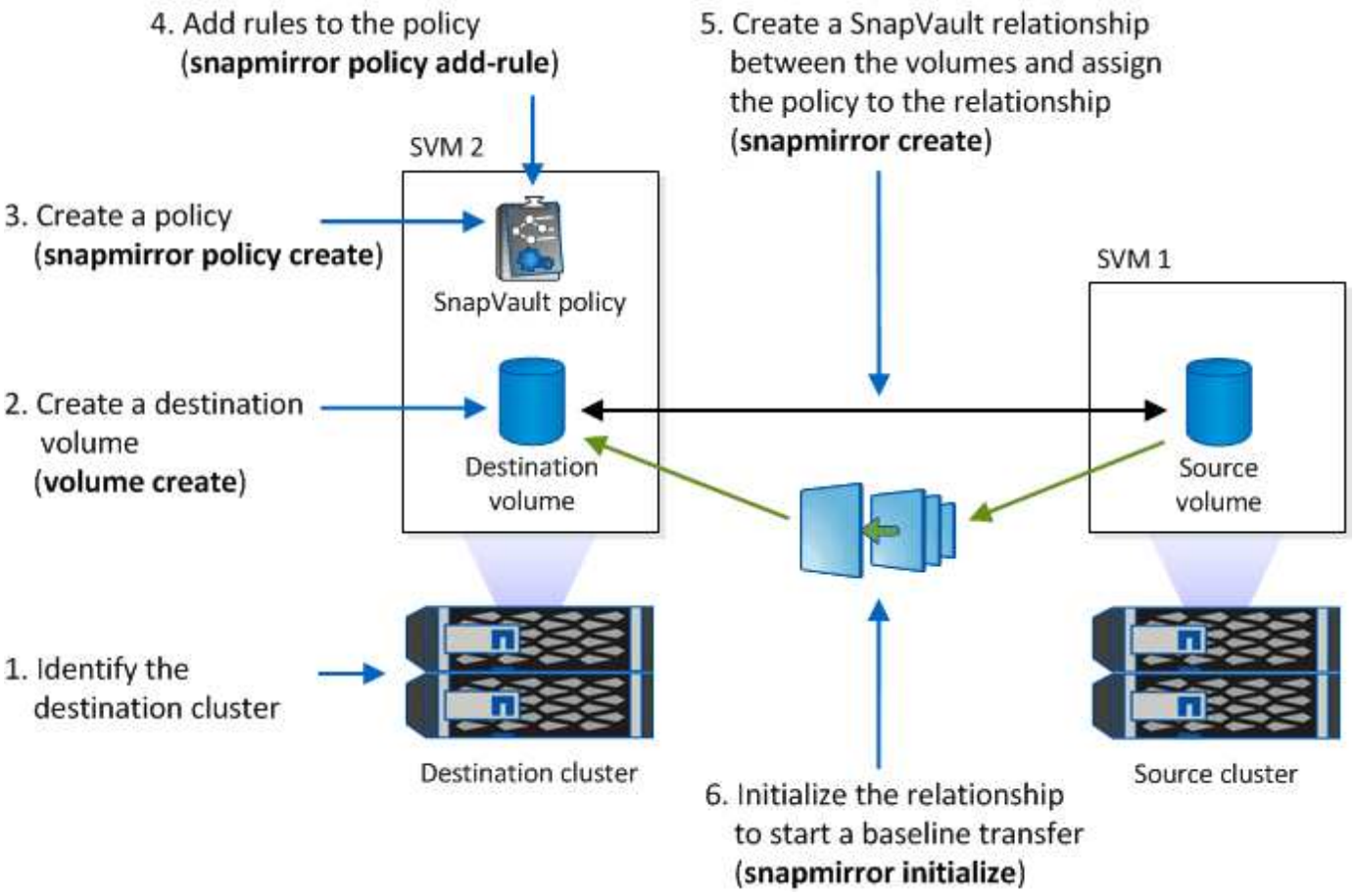
A partir do ONTAP 9.14.1, é possível especificar períodos de retenção para rótulos SnapMirror específicos na política SnapMirror da relação SnapMirror para que os snapshots replicados da origem para o volume de destino sejam retidos pelo período de retenção especificado na regra. Se nenhum período de retenção for especificado, o período de retenção padrão do volume de destino será usado.

A partir do ONTAP 9.13.1, é possível restaurar instantaneamente um instantâneo bloqueado no volume SnapLock de destino de uma relação de Vault do SnapLock criando um FlexClone com a `snaplock-type` opção definida `non-snaplock` e especificando o instantâneo como o "pai-instantâneo" ao executar a operação de criação de clone de volume. Saiba mais "Criando um volume FlexClone com um tipo SnapLock"sobre o .

Para configurações do MetroCluster, você deve estar ciente do seguinte:

- Você pode criar uma relação do SnapVault apenas entre SVMs de origem sincronizada, e não entre uma SVM de origem sincronizada e um SVM de destino sincronizado.
- Você pode criar uma relação de SnapVault a partir de um volume em uma SVM de origem sincronizada até um SVM de fornecimento de dados.
- Você pode criar uma relação de SnapVault de um volume em uma SVM de fornecimento de dados a um volume de DP em uma fonte sincronizada SVM.

A ilustração a seguir mostra o procedimento para inicializar um relacionamento de Vault do SnapLock:



Passos

Você pode usar a CLI do ONTAP para criar uma relação de cofre do SnapLock ou, a partir do ONTAP 9.15,1, você pode usar o Gerenciador do sistema para criar uma relação de cofre do SnapLock.

System Manager

1. Navegue até **Storage > volumes** e selecione **Add**.
2. Na janela **Adicionar volume**, escolha **mais opções**.
3. Introduza o nome do volume, o tamanho, a política de exportação e o nome da partilha.
4. Selecione **Bloquear instantâneos de destino para evitar a exclusão** e, na seção **método de bloqueio**, escolha **SnapLock for SnapVault**. Esta seleção não é exibida se o tipo de diretiva selecionado não for do tipo "Vault", se a licença SnapLock não estiver instalada ou se o Relógio de conformidade não for inicializado.
5. Se ainda não estiver ativado, selecione **Inicializar Relógio SnapLock Compliance**.
6. Salve suas alterações.

CLI

1. No cluster de destino, crie um volume do tipo de destino SnapLock `DP` igual ou superior ao volume de origem:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise> -type DP
   -size <size>
   ```

   O comando a seguir cria um volume 2GBD SnapLock Compliance nomeado `dstvolB` no `SVM2` agregado `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

2. No cluster de destino, "defina o período de retenção padrão".
3. "Crie uma nova relação de replicação" Entre a fonte que não é SnapLock e o novo destino SnapLock que você criou.

   Este exemplo cria uma nova relação SnapMirror com o volume SnapLock de destino `dstvolB` usando uma política de `XDPDefault` para Vault snapshots rotulados diariamente e semanalmente em uma programação por hora:

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

   > "Crie uma política de replicação personalizada" ou a "programação personalizada" se os padrões disponíveis não forem adequados.

4. No SVM de destino, inicialize a relação SnapVault criada:

   ```
   snapmirror initialize -destination-path <destination_path>
   ```

O comando a seguir inicializa a relação entre o volume de origem `srcvolA` ligado `SVM1` e o volume de destino `dstvolB` no `SVM2`:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. Depois que a relação for inicializada e ociosa, use o `snapshot show` comando no destino para verificar o tempo de expiração do SnapLock aplicado aos snapshots replicados.

   Este exemplo lista os instantâneos no volume `dstvolB` que têm o rótulo SnapMirror e a data de expiração do SnapLock:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

Informações relacionadas

"Peering de cluster e SVM"

"Backup de volume usando o SnapVault"

Espelhar arquivos WORM para recuperação de desastres

Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres e outros fins. O volume de origem e o volume de destino devem ser configurados para o SnapLock, e ambos os volumes devem ter o mesmo modo SnapLock, conformidade ou empresa. Todas as principais propriedades SnapLock do volume e dos arquivos são replicadas.

Pré-requisitos

Os volumes de origem e destino devem ser criados em clusters com SVMs com peered. Para obter mais informações, "Peering de cluster e SVM"consulte .

Sobre esta tarefa

- A partir do ONTAP 9.5, você pode replicar arquivos WORM com a relação SnapMirror do tipo XDP (proteção de dados estendida) em vez da relação de tipo DP (proteção de dados). O modo XDP é independente da versão do ONTAP e é capaz de diferenciar arquivos armazenados no mesmo bloco, facilitando a ressincronização de volumes replicados em modo de conformidade. Para obter informações sobre como converter uma relação de tipo DP existente em uma relação do tipo XDP, "Proteção de dados"consulte .
- Uma operação ressincronizada em uma relação de SnapMirror tipo DP falha para um volume de modo de conformidade se o SnapLock determinar que isso resultará em perda de dados. Se uma operação ressincronizada falhar, você pode usar o `volume clone create` comando para fazer um clone do volume de destino. Em seguida, é possível sincronizar novamente o volume de origem com o clone.
- Uma relação SnapMirror do tipo XDP entre volumes compatíveis com SnapLock suporta uma ressincronização após uma pausa, mesmo que os dados no destino tenham divergido da origem após a quebra.

Em uma ressincronização, quando a divergência de dados é detetada entre a origem do destino além do snapshot comum, um novo snapshot é cortado no destino para capturar essa divergência. O novo snapshot e o snapshot comum são bloqueados com um tempo de retenção da seguinte forma:

- O tempo de expiração do volume do destino
- Se o tempo de expiração do volume estiver no passado ou não tiver sido definido, o instantâneo será bloqueado por um período de 30 dias
- Se o destino tiver retenção legal, o período de expiração do volume real é mascarado e aparece como "indefinido"; no entanto, o instantâneo é bloqueado durante o período de expiração do volume real.

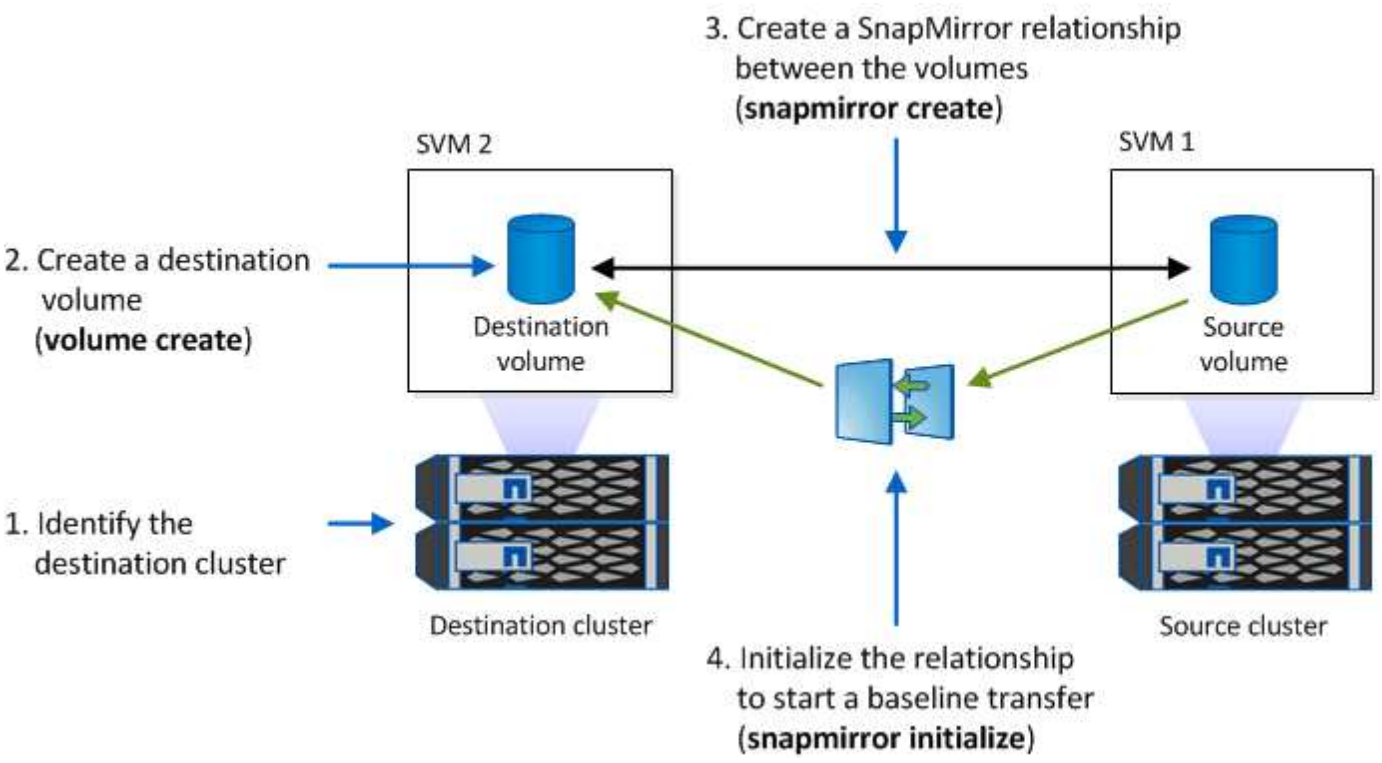
Se o volume de destino tiver um período de expiração posterior à origem, o período de expiração do destino será retido e não será substituído pelo período de expiração do volume de origem após a ressincronização.

Se o destino tiver retenções legais que diferem da origem, não é permitido fazer uma ressincronização. A origem e o destino devem ter retenção legal idêntica ou todas as retenção legal no destino devem ser liberadas antes de uma ressincronização ser tentada.

Uma cópia Snapshot bloqueada no volume de destino criada para capturar os dados divergentes pode ser copiada para a origem usando a CLI executando o `snapmirror update -s snapshot` comando. O instantâneo uma vez copiado continuará a ser bloqueado na origem também.

- As relações de proteção de dados do SVM não são compatíveis.
- Relacionamentos de proteção de dados de compartilhamento de carga não são suportados.

A ilustração a seguir mostra o procedimento para inicializar uma relação SnapMirror:



System Manager

A partir do ONTAP 9.12,1, você pode usar o System Manager para configurar a replicação do SnapMirror de arquivos WORM.

Passos

1. Navegue até **Storage > volumes**.
2. Clique em **Mostrar/Ocultar** e selecione **tipo SnapLock** para exibir a coluna na janela **volumes**.
3. Localize um volume SnapLock.
4. Clique ⋮ e selecione **Protect**.
5. Escolha o cluster de destino e a VM de armazenamento de destino.
6. Clique em **mais opções**.
7. Selecione **Mostrar políticas legadas** e selecione **DPDefault (legacy)**.
8. Na seção **Detalhes da Configuração do destino**, selecione **Substituir agendamento de transferência** e selecione **hora a hora**.
9. Clique em **Salvar**.
10. À esquerda do nome do volume de origem, clique na seta para expandir os detalhes do volume e, no lado direito da página, revise os detalhes de proteção SnapMirror remota.
11. No cluster remoto, navegue até **relacionamentos de proteção**.
12. Localize a relação e clique no nome do volume de destino para visualizar os detalhes da relação.
13. Verifique se o tipo de SnapLock do volume de destino e outras informações do SnapLock.

CLI

1. Identificar o cluster de destino.
2. No cluster de destino, "Instale a licença SnapLock" "Inicialize o Relógio de conformidade", e, se estiver a utilizar uma versão do ONTAP anterior a 9.10.1, "Crie um agregado SnapLock".
3. No cluster de destino, crie um volume de tipo de destino SnapLock `DP` com o mesmo tamanho ou maior do que o volume de origem:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > ⓘ A partir do ONTAP 9.10,1, os volumes SnapLock e não SnapLock podem existir no mesmo agregado; portanto, você não será mais necessário criar um agregado SnapLock separado se estiver usando o ONTAP 9.10,1. Você usa a opção volume -SnapLock-type para especificar um tipo de volume Compliance ou Enterprise SnapLock. Em versões do ONTAP anteriores ao ONTAP 9.10,1, o modo SnapLock --conformidade ou empresa — é herdado do agregado. Os volumes de destino flexíveis de versão não são suportados. A definição de idioma do volume de destino tem de corresponder à definição de idioma do volume de origem.

   O comando a seguir cria um volume SnapLock de 2 GB `Compliance` nomeado `dstvolB SVM2` no agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. No SVM de destino, crie uma política de SnapMirror:

   `snapmirror policy create -vserver SVM_name -policy policy_name`

   O comando a seguir cria a política toda a SVM `SVM1-mirror` :

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. No SVM de destino, crie um agendamento do SnapMirror:

   `job schedule cron create -name schedule_name -dayofweek day_of_week -hour hour -minute minute`

   O comando a seguir cria uma programação SnapMirror chamada `weekendcron`:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. No SVM de destino, crie uma relação SnapMirror:

   `snapmirror create -source-path source_path -destination-path destination_path -type XDP|DP -policy policy_name -schedule schedule_name`

   O comando a seguir cria uma relação SnapMirror entre o volume de origem `srcvolA` ligado `SVM1` e o volume de destino ligado `SVM2` e `dstvolB` atribui a política `SVM1-mirror` e a programação `weekendcron`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   O tipo XDP está disponível no ONTAP 9.5 e posterior. Você deve usar o tipo DP no ONTAP 9.4 e anterior.

7. No SVM de destino, inicialize a relação SnapMirror:

   `snapmirror initialize -destination-path destination_path`

   O processo de inicialização executa uma *transferência de linha de base* para o volume de destino. O SnapMirror faz uma cópia Snapshot do volume de origem e transfere a cópia e todos os blocos de dados que ele faz referência ao volume de destino. Ele também transfere quaisquer outras cópias Snapshot no volume de origem para o volume de destino.

O comando a seguir inicializa a relação entre o volume de origem `srcvolA` ligado `SVM1` e o volume de destino `dstvolB` no `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Informações relacionadas

"Peering de cluster e SVM"

"Preparação para recuperação de desastres em volume"

"Proteção de dados"

Retenha arquivos WORM durante o litígio usando retenção legal

A partir do ONTAP 9.3, você pode reter arquivos WORM em modo de conformidade durante um litígio usando o recurso *retenção legal*.

Antes de começar

- Você deve ser um administrador do SnapLock para executar esta tarefa.

  "Crie uma conta de administrador do SnapLock"

- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Sobre esta tarefa

Um arquivo sob uma retenção legal se comporta como um arquivo WORM com um período de retenção indefinido. É da sua responsabilidade especificar quando o período de retenção Legal termina.

O número de arquivos que você pode colocar em uma retenção legal depende do espaço disponível no volume.

Passos

1. Iniciar uma retenção legal:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   O comando a seguir inicia uma retenção Legal para todos os arquivos no `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Terminar uma retenção legal:

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   O comando a seguir termina uma retenção Legal para todos os arquivos no `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Exclua a visão geral de arquivos WORM

Você pode excluir arquivos WORM do modo empresarial durante o período de retenção usando o recurso de exclusão privilegiada. Antes de poder utilizar esta funcionalidade, tem de criar uma conta de administrador do SnapLock e, em seguida, utilizar a conta, ativar a funcionalidade.

Crie uma conta de administrador do SnapLock

Você deve ter o administrador do SnapLock Privileges para executar uma exclusão privilegiada. Esses Privileges são definidos na função vsadmin-SnapLock. Se ainda não tiver sido atribuída essa função, você poderá solicitar ao administrador do cluster que crie uma conta de administrador SVM com a função de administrador do SnapLock.

O que você vai precisar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Passos

1. Crie uma conta de administrador do SVM com a função de administrador do SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   O comando a seguir permite que a conta de administrador SVM `SnapLockAdmin` com a função predefinida `vsadmin-snaplock` acesse `SVM1` usando uma senha:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

Ative o recurso de exclusão privilegiada

Você deve habilitar explicitamente o recurso de exclusão privilegiada no volume Enterprise que contém os arquivos WORM que você deseja excluir.

Sobre esta tarefa

O valor `-privileged-delete` da opção determina se a exclusão privilegiada está ativada. Os valores possíveis são `enabled`, `disabled`, e `permanently-disabled`.

`permanently-disabled` é o estado do terminal. Não é possível ativar a exclusão privilegiada no volume depois de definir o estado como `permanently-disabled`.

Passos

1. Ativar exclusão privilegiada para um volume SnapLock Enterprise:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   O comando a seguir habilita o recurso de exclusão privilegiada para o volume Enterprise `dataVol` `SVM1` no :

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
-delete enabled
```

Exclua arquivos WORM do modo empresarial

Você pode usar o recurso de exclusão privilegiada para excluir arquivos WORM do modo empresarial durante o período de retenção.

O que você vai precisar

- Você deve ser um administrador do SnapLock para executar esta tarefa.
- Você deve ter criado um log de auditoria do SnapLock e habilitado o recurso de exclusão privilegiada no volume empresa.

Sobre esta tarefa

Não é possível usar uma operação de exclusão privilegiada para excluir um arquivo WORM expirado. Use o `volume file retention show` comando para visualizar o tempo de retenção do arquivo WORM que você deseja excluir. Para obter mais informações, consulte a página man para o comando.

Passo

1. Excluir um arquivo WORM em um volume empresarial:

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   O comando a seguir exclui o arquivo `/vol/dataVol/f1` no SVM`SVM1`:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

Mover um volume SnapLock

A partir do ONTAP 9.8, é possível mover um volume SnapLock para um agregado de destino do mesmo tipo, seja empresa para empresa ou conformidade com a

conformidade. Você deve ter a função de segurança do SnapLock para mover um volume do SnapLock.

Crie uma conta de administrador de segurança do SnapLock

Você deve ter o administrador de segurança do SnapLock Privileges para executar uma movimentação de volume do SnapLock. Este privilégio é concedido a você com a função *SnapLock*, introduzida no ONTAP 9.8. Se ainda não tiver sido atribuída essa função, pode pedir ao administrador do cluster para criar um utilizador de segurança do SnapLock com esta função de segurança do SnapLock.

O que você vai precisar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve ter feito login em uma conexão segura (SSH, console ou ZAPI).

Sobre esta tarefa

A função SnapLock está associada ao administrador SVM, diferentemente da função vsadmin-SnapLock, que é associada ao SVM de dados.

Passo

1. Crie uma conta de administrador do SVM com a função de administrador do SnapLock:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   O comando a seguir permite que a conta de administrador SVM `SnapLockAdmin` com a função predefinida `snaplock` acesse o administrador SVM `cluster1` usando uma senha:

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

Mover um volume SnapLock

Você pode usar o `volume move` comando para mover um volume SnapLock para um agregado de destino.

O que você vai precisar

- Você precisa ter criado um log de auditoria protegido pela SnapLock antes de executar a movimentação de volume do SnapLock.

  "Criar um log de auditoria".

- Se você estiver usando uma versão do ONTAP anterior à ONTAP 9.10,1, o agregado de destino deve ser o mesmo tipo de SnapLock que o volume do SnapLock que deseja mover, seja de conformidade ou de empresa para empresa. A partir do ONTAP 9.10,1, essa restrição é removida e um agregado pode incluir volumes de Compliance e Enterprise SnapLock, bem como volumes que não são SnapLock.
- Você deve ser um usuário com a função de segurança do SnapLock.

Passos

1. Usando uma conexão segura, faça login no LIF de gerenciamento de clusters do ONTAP:

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Mover um volume SnapLock:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
-aggregate destination_aggregate_name
```

3. Verificar o estado da operação de deslocação do volume:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
volume,phase,vserver
```

Bloqueie uma cópia Snapshot para proteção contra ataques de ransomware

A partir do ONTAP 9.12,1, você pode bloquear uma cópia Snapshot em um volume que não seja da SnapLock para proteger contra ataques de ransomware. Bloquear cópias Snapshot garante que elas não podem ser excluídas acidentalmente ou maliciosamente.

Você usa o recurso de relógio SnapLock Compliance para bloquear cópias snapshot por um período especificado, de modo que elas não possam ser excluídas até que o tempo de expiração seja atingido. O bloqueio de cópias Snapshot faz com que elas sejam protegidas contra ameaças de ransomware. Use cópias Snapshot bloqueadas para recuperar dados se um volume for comprometido por um ataque de ransomware.

A partir do ONTAP 9.14,1, o bloqueio de cópias Snapshot é compatível com a retenção de longo prazo de cópias Snapshot em destinos de cofres do SnapLock e em volumes de destino que não sejam da SnapLock SnapMirror. O bloqueio de cópias snapshot é ativado definindo o período de retenção usando regras de política do SnapMirror associadas a um etiqueta de política existente. A regra substitui o período de retenção padrão definido no volume. Se não houver período de retenção associado ao rótulo SnapMirror, o período de retenção padrão do volume será usado.

Requisitos e considerações da cópia Snapshot à prova de violações

- Se você estiver usando a CLI do ONTAP, todos os nós do cluster devem estar executando o ONTAP 9.12,1 ou posterior. Se você estiver usando o Gerenciador de sistema, todos os nós devem estar executando o ONTAP 9.13,1 ou posterior.
- "A licença SnapLock deve ser instalada no cluster". Esta licença está incluída no "ONTAP One".
- "O relógio de conformidade no cluster deve ser inicializado".
- Quando o bloqueio de snapshot está ativado em um volume, é possível atualizar os clusters para uma versão do ONTAP posterior à ONTAP 9.12,1. No entanto, não é possível reverter para uma versão anterior do ONTAP até que todas as cópias Snapshot bloqueadas atinjam a data de expiração e sejam excluídas e o bloqueio de cópias snapshot seja desativado.
- Quando um instantâneo é bloqueado, o tempo de expiração do volume é definido para o tempo de expiração da cópia Snapshot. Se mais de uma cópia Snapshot estiver bloqueada, o tempo de expiração do volume refletirá o maior tempo de expiração dentre todas as cópias Snapshot.
- O período de retenção para cópias Snapshot bloqueadas tem precedência sobre a contagem de manutenção da cópia Snapshot, o que significa que o limite de contagem de retenção não será honrado se o período de retenção da cópia Snapshot para cópias Snapshot bloqueadas não tiver expirado.
- Em um relacionamento do SnapMirror, você pode definir um período de retenção em uma regra de política de cofre de espelho e o período de retenção é aplicado para cópias Snapshot replicadas no destino se o volume de destino tiver o bloqueio de cópias Snapshot ativado. O período de retenção tem precedência sobre a contagem de manutenção; por exemplo, as cópias Snapshot que não passaram em sua expiração

serão mantidas mesmo que a contagem de manutenção seja excedida.

- Você pode renomear uma cópia Snapshot em um volume que não seja SnapLock. As operações de renomeação de snapshot no volume primário de uma relação de SnapMirror são refletidas no volume secundário somente se a política for EspelrorAllinstantâneos. Para outros tipos de diretiva, a cópia Snapshot renomeada não é propagada durante as atualizações.
- Se você estiver usando a CLI do ONTAP, poderá restaurar uma cópia Snapshot bloqueada com o `volume snapshot restore` comando somente se a cópia Snapshot bloqueada for a mais recente. Se houver cópias Snapshot não expiradas depois da restauração, a operação de restauração da cópia Snapshot falhará.

Recursos compatíveis com cópias Snapshot à prova de violações

- "Cloud Volumes ONTAP"
- Volumes FlexGroup

  O bloqueio de cópias snapshot é compatível com volumes FlexGroup. O bloqueio instantâneo ocorre apenas na cópia Snapshot constituinte raiz. A exclusão do volume FlexGroup só é permitida se o tempo de expiração do componente raiz tiver passado.

- Conversão de FlexVol para FlexGroup

  Você pode converter um FlexVol volume com cópias Snapshot bloqueadas em um volume FlexGroup. As cópias snapshot permanecem bloqueadas após a conversão.

- Clone de volume e clone de arquivo

  Você pode criar clones de volume e clones de arquivos a partir de uma cópia Snapshot bloqueada.

Funcionalidades não suportadas

No momento, os recursos a seguir não são compatíveis com cópias Snapshot à prova de violações:

- Grupos de consistência
- FabricPool
- Volumes FlexCache
- SMtape
- Sincronização ativa do SnapMirror
- Regras de política do SnapMirror usando o `-schedule` parâmetro
- SnapMirror síncrono
- Mobilidade de dados SVM (usada para migrar ou realocar um SVM de um cluster de origem para um cluster de destino)

Ative o bloqueio de cópias instantâneas ao criar um volume

A partir do ONTAP 9.12,1, é possível ativar o bloqueio de cópias instantâneas ao criar um novo volume ou ao modificar um volume existente usando a `-snapshot-locking-enabled` opção com `volume create` os comandos e `volume modify` na CLI. A partir do ONTAP 9.13,1, você pode usar o Gerenciador do sistema para ativar o bloqueio de cópias instantâneas.

System Manager

1. Navegue até **Storage > volumes** e selecione **Add**.
2. Na janela **Adicionar volume**, escolha **mais opções**.
3. Introduza o nome do volume, o tamanho, a política de exportação e o nome da partilha.
4. Selecione **Ativar bloqueio instantâneo**. Esta seleção não é apresentada se a licença SnapLock não estiver instalada.
5. Se ainda não estiver ativado, selecione **Inicializar Relógio SnapLock Compliance**.
6. Salve suas alterações.
7. Na janela **volumes**, selecione o volume que você atualizou e escolha **Visão geral**.
8. Verifique se **SnapLock Snapshot Copy Locking** é exibido como **Enabled**.

CLI

1. Para criar um novo volume e habilitar o bloqueio de cópias instantâneas, digite o seguinte comando:

   ```
   volume create -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

   O comando a seguir habilita o bloqueio de cópias snapshot em um novo volume chamado vol1:

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Habilite o bloqueio de cópias snapshot em um volume existente

A partir do ONTAP 9.12,1, é possível ativar o bloqueio de cópias snapshot em um volume existente usando a CLI do ONTAP. A partir do ONTAP 9.13,1, você pode usar o Gerenciador do sistema para ativar o bloqueio de cópias instantâneas em um volume existente.

System Manager

1. Navegue até **Storage > volumes**.
2. Selecione ⋮ e escolha **Editar > volume**.
3. Na janela **Editar volume**, localize a seção Configurações de cópias instantâneas (locais) e selecione **Ativar bloqueio instantâneo**.

   Esta seleção não é apresentada se a licença SnapLock não estiver instalada.
4. Se ainda não estiver ativado, selecione **Inicializar Relógio SnapLock Compliance**.
5. Salve suas alterações.
6. Na janela **volumes**, selecione o volume que você atualizou e escolha **Visão geral**.
7. Verifique se **SnapLock Snapshot Copy Locking** é exibido como **Enabled**.

CLI

1. Para modificar um volume existente para habilitar o bloqueio de cópias instantâneas, digite o seguinte comando:

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

Crie uma política de cópia Snapshot bloqueada e aplique retenção

A partir do ONTAP 9.12,1, você pode criar políticas de cópia Snapshot para aplicar um período de retenção de cópia Snapshot e aplicar a política a um volume para bloquear cópias Snapshot pelo período especificado. Você também pode bloquear uma cópia Snapshot definindo manualmente um período de retenção. A partir do ONTAP 9.13,1, você pode usar o Gerenciador do sistema para criar políticas de bloqueio de cópias Snapshot e aplicá-las a um volume.

Criar uma política de bloqueio de cópias Snapshot

System Manager

1. Navegue até **Storage > Storage VMs** e selecione uma VM de armazenamento.
2. Selecione **Definições**.
3. Localize **políticas de instantâneos** e →selecione .
4. Na janela **Add Snapshot Policy** (Adicionar política de instantâneo*), introduza o nome da política.
5. + Add Selecione .
6. Forneça os detalhes da programação da cópia Snapshot, incluindo o nome da programação, o máximo de cópias snapshot a serem mantidas e o período de retenção da SnapLock.
7. Na coluna **período de retenção do SnapLock**, insira o número de horas, dias, meses ou anos para reter as cópias do Snapshot. Por exemplo, uma política de cópia Snapshot com um período de retenção de 5 dias bloqueia uma cópia Snapshot por 5 dias a partir do momento em que é criada, e não pode ser excluída durante esse período. Os seguintes intervalos de período de retenção são suportados:
   - Anos: 0 - 100
   - Meses: 0 - 1200
   - Dias: 0 - 36500
   - Horário: 0h - 24H.
8. Salve suas alterações.

CLI

1. Para criar uma política de cópia Snapshot, digite o seguinte comando:

   ```
   volume snapshot policy create -policy policy_name -enabled true -schedule1
   schedule1_name -count1 maximum_Snapshot_copies -retention-period1
   _retention_period
   ```

   O comando a seguir cria uma política de bloqueio de cópia Snapshot:

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   Uma cópia Snapshot não será substituída se estiver sob retenção ativa; ou seja, a contagem de retenção não será honrada se houver cópias Snapshot bloqueadas que ainda não tenham expirado.

Aplique uma política de bloqueio a um volume

System Manager

1. Navegue até **Storage > volumes**.
2. Selecione ⋮ e escolha **Editar > volume**.
3. Na janela **Editar volume**, selecione **Agendar cópias instantâneas**.
4. Selecione a política de bloqueio de cópia Snapshot na lista.
5. Se o bloqueio de cópias instantâneas não estiver ativado, selecione **Ativar bloqueio instantâneo**.
6. Salve suas alterações.

CLI

1. Para aplicar uma política de bloqueio de cópia Snapshot a um volume existente, digite o seguinte comando:

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

Aplicar período de retenção durante a criação da cópia Snapshot manual

Você pode aplicar um período de retenção da cópia Snapshot ao criar manualmente uma cópia Snapshot. O bloqueio de cópias snapshot deve estar ativado no volume; caso contrário, a configuração do período de retenção é ignorada.

System Manager

1. Navegue até **Storage > volumes** e selecione um volume.
2. Na página de detalhes do volume, selecione a guia **cópias instantâneas**.
3. + Add Selecione .
4. Insira o nome da cópia Snapshot e o tempo de expiração do SnapLock. Você pode selecionar o calendário para escolher a data e a hora de expiração da retenção.
5. Salve suas alterações.
6. Na página **volumes > cópias Snapshot**, selecione **Mostrar/Ocultar** e escolha **tempo de expiração do SnapLock** para exibir a coluna **tempo de expiração do SnapLock** e verifique se o tempo de retenção está definido.

CLI

1. Para criar uma cópia Snapshot manualmente e aplicar um período de retenção de bloqueio, digite o seguinte comando:

   `volume snapshot create -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-snaplock-expiry-time` *`expiration_date_time`*

   O comando a seguir cria uma nova cópia Snapshot e define o período de retenção:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Aplicar um período de retenção a uma cópia Snapshot existente

System Manager

1. Navegue até **Storage > volumes** e selecione um volume.
2. Na página de detalhes do volume, selecione a guia **cópias instantâneas**.
3. Selecione a cópia Snapshot, selecione ⋮ e escolha **Modificar tempo de expiração do SnapLock**. Você pode selecionar o calendário para escolher a data e a hora de expiração da retenção.
4. Salve suas alterações.
5. Na página **volumes > cópias Snapshot**, selecione **Mostrar/Ocultar** e escolha **tempo de expiração do SnapLock** para exibir a coluna **tempo de expiração do SnapLock** e verifique se o tempo de retenção está definido.

CLI

1. Para aplicar manualmente um período de retenção a uma cópia Snapshot existente, digite o seguinte comando:

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   O exemplo a seguir aplica um período de retenção a uma cópia Snapshot existente:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Modificar uma política existente para aplicar retenção a longo prazo

Em um relacionamento do SnapMirror, você pode definir um período de retenção em uma regra de política de cofre de espelho e o período de retenção é aplicado para cópias Snapshot replicadas no destino se o volume de destino tiver o bloqueio de cópias Snapshot ativado. O período de retenção tem precedência sobre a contagem de manutenção; por exemplo, as cópias Snapshot que não passaram em sua expiração serão mantidas mesmo que a contagem de manutenção seja excedida.

A partir do ONTAP 9.14,1, é possível modificar uma política SnapMirror existente adicionando uma regra para definir a retenção a longo prazo das cópias Snapshot. A regra é usada para substituir o período de retenção de volume padrão nos destinos do Vault do SnapLock e em volumes de destino que não sejam do SnapLock SnapMirror.

1. Adicionar uma regra a uma política SnapMirror existente:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of Snapshot copies> -retention
   -period [<integer> days|months|years]
   ```

   O exemplo a seguir cria uma regra que aplica um período de retenção de 6 meses à política existente chamada "lockvault":

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

APIs da SnapLock

Você pode usar APIs Zephyr para integrar com a funcionalidade SnapLock em scripts ou automação de fluxo de trabalho. As APIs usam mensagens XML em HTTP, HTTPS e Windows DCE/RPC. Saiba mais no "Documentação de automação do ONTAP".

interrupção de impressão digital de ficheiros

Abortar uma operação de impressão digital do ficheiro.

file-fingerprint-dump

Exibir informações de impressão digital do arquivo.

file-fingerprint-get-iter

Exibir o status das operações de impressão digital do arquivo.

ficheiro-impressão digital-iniciar

Gerar uma impressão digital de arquivo.

SnapLock-archive-vserver-log

Arquive o arquivo de log de auditoria ativo.

SnapLock-create-vserver-log

Criar uma configuração de log de auditoria para um SVM.

SnapLock-delete-vserver-log

Excluir uma configuração de log de auditoria de um SVM.

SnapLock-file-privileged-delete

Execute uma operação de exclusão privilegiada.

retenção de arquivos-get-SnapLock

Obtenha o período de retenção de um arquivo.

SnapLock-get-node-compliance-clock

Obtenha a data e a hora do nó ComplianceClock.

SnapLock-get-vserver-ative-log-files-iter

Apresentar o estado dos ficheiros de registo ativos.

SnapLock-get-vserver-log-iter

Exibir a configuração do log de auditoria.

SnapLock-modify-vserver-log

Modificar a configuração do log de auditoria de um SVM.

retenção de arquivo-conjunto-SnapLock

Defina o tempo de retenção para um arquivo.

relógio de conformidade do nó definido por SnapLock

Defina a data e a hora do nó ComplianceClock.

SnapLock-volume-set-privileged-delete

Defina a opção de exclusão privilegiada em um volume SnapLock Enterprise.

volume-get-SnapLock-attrs

Obtenha os atributos de um volume SnapLock.

volume-set-SnapLock-attrs

Defina os atributos de um volume SnapLock.

Grupos de consistência

Visão geral dos grupos de consistência

Um grupo de consistência é uma coleção de volumes que são gerenciados como uma única unidade. No ONTAP, os grupos de consistência fornecem gerenciamento fácil e uma garantia de proteção para um workload de aplicações que abrange vários volumes.

Use grupos de consistência para simplificar o gerenciamento de storage. Imagine que você tem um banco de dados importante abrangendo vinte LUNs. Você pode gerenciar os LUNs individualmente ou tratar os LUNs como um conjunto de dados solitário, organizando-os em um único grupo de consistência.

Grupos de consistência facilitam o gerenciamento do workload de aplicações, com políticas de proteção locais e remotas facilmente configuradas e cópias Snapshot simultâneas de uma coleção de volumes em um momento consistente com falhas ou consistentes com aplicações. As cópias snapshot de um grupo de consistência permitem a restauração do workload de uma aplicação inteira.

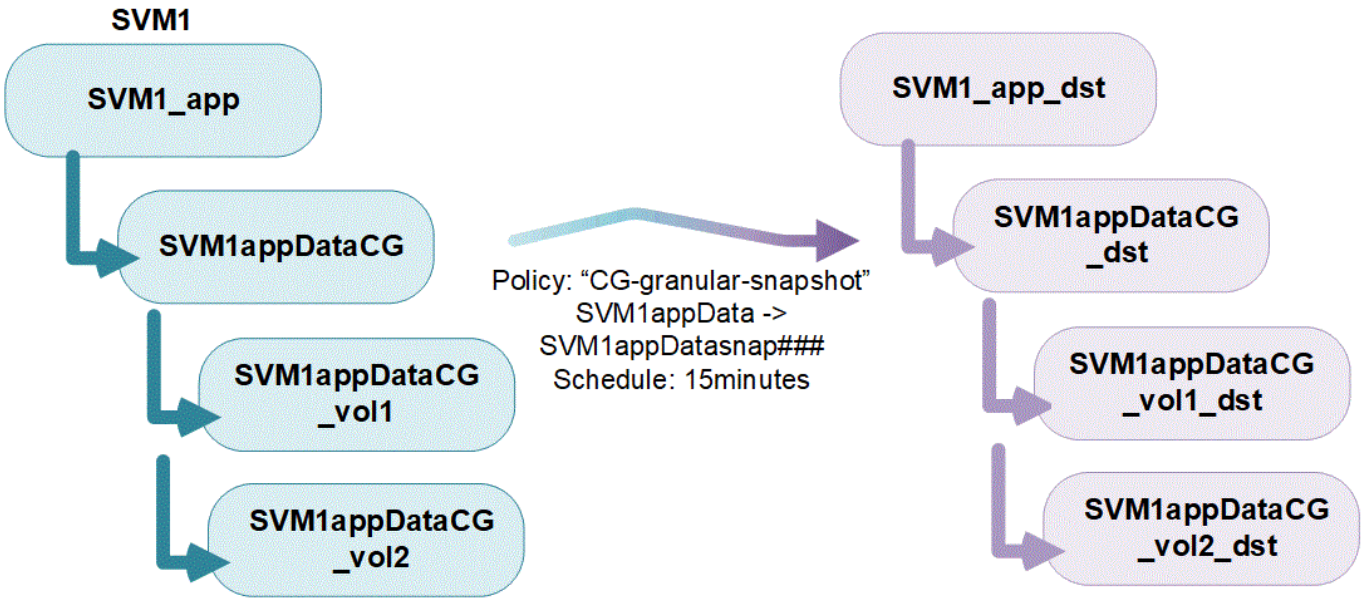
Saiba mais sobre grupos de consistência

Os grupos de consistência são compatíveis com qualquer FlexVol volume, independentemente do protocolo (nas, SAN ou NVMe) e podem ser gerenciados pela API REST do ONTAP ou no Gerenciador de sistema no item de menu **armazenamento > grupos de consistência**. A partir do ONTAP 9.14,1, os grupos de consistência podem ser gerenciados com a CLI do ONTAP.

Grupos de consistência podem existir como entidades individuais - como uma coleção de volumes - ou em uma relação hierárquica, que consiste em outros grupos de consistência. Os volumes individuais podem ter sua própria política de Snapshot granular de volume. Além disso, pode haver uma política de Snapshot em todo o grupo de consistência. O grupo de consistência só pode ter uma relação de sincronização ativa do SnapMirror e uma política SnapMirror compartilhada, que pode ser usada para recuperar todo o grupo de

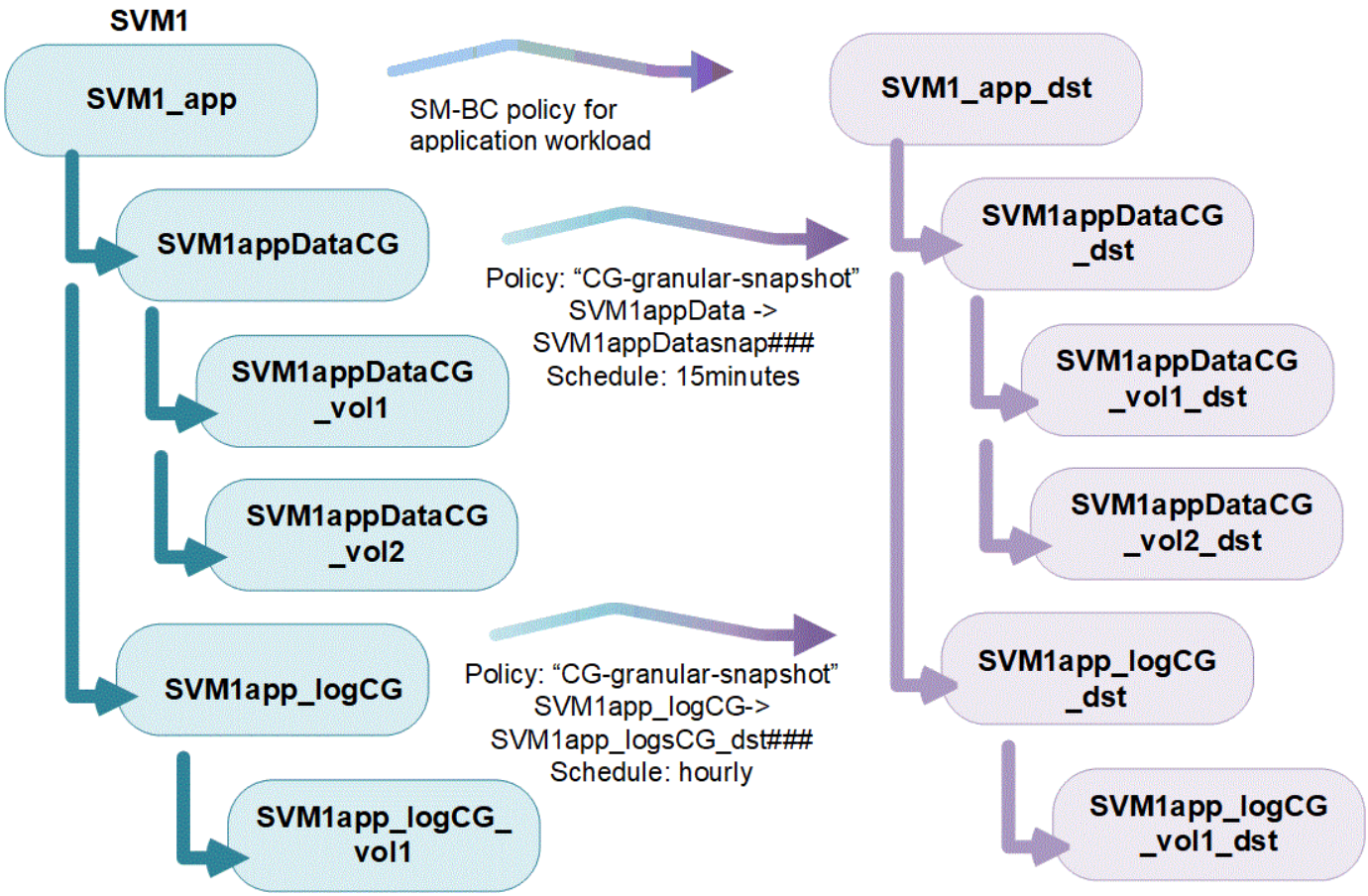
consistência.

O diagrama a seguir ilustra como você pode usar um grupo de consistência individual. Os dados de um aplicativo hospedado em `SVM1` dois volumes: `vol1` E `vol2`. Uma política de Snapshot no grupo de consistência captura cópias Snapshot dos dados a cada 15 minutos.



Workloads de aplicações maiores podem exigir vários grupos de consistência. Nessas situações, você pode criar grupos hierárquicos de consistência, em que um único grupo de consistência se torna os componentes filhos de um grupo de consistência pai. O grupo de consistência pai pode incluir até cinco grupos filhos. Assim como em grupos de consistência individuais, uma política de proteção de sincronização ativa remota do SnapMirror pode ser aplicada a toda a configuração de grupos de consistência (pai e filhos) para recuperar a carga de trabalho do aplicativo.

No exemplo a seguir, um aplicativo é hospedado no `SVM1`. O administrador criou um grupo de consistência pai `SVM1_app` , que inclui dois grupos filhos de consistência: `SVM1appDataCG` Para os dados e `SVM1app_logCG` para os logs. Cada grupo de consistência filho tem sua própria política do Snapshot. Cópias snapshot dos volumes `SVM1appDataCG` são realizadas a cada 15 minutos. Os instantâneos de `SVM1app_logCG` são tirados por hora. O grupo de consistência pai `SVM1_app` tem uma política de sincronização ativa do SnapMirror que replica os dados para garantir a continuidade do serviço em caso de desastre.



A partir do ONTAP 9.12,1, os grupos de consistência suportam clonagem e modificam os membros da consistência no adicionar ou remover volumesGerenciador do sistema e na API REST do ONTAP. A partir do ONTAP 9.12,1, a API REST do ONTAP também suporta:

- Criação de grupos de consistência com novos volumes NFS, SMB ou namespaces NVMe.
- Adição de volumes NFS, SMB ou namespaces NVMe novos ou existentes a grupos de consistência existentes.

Para obter mais informações sobre a API REST do ONTAP, "Documentação de referência da API REST do ONTAP" consulte .

Monitorar grupos de consistência

A partir do ONTAP 9.13,1, os grupos de consistência oferecem monitoramento de capacidade e desempenho em tempo real e histórico, oferecendo insights sobre o desempenho de aplicativos e grupos de consistência individuais.

Os dados de monitoramento são atualizados a cada cinco minutos e são mantidos por até um ano. Você pode acompanhar as métricas de:

- Performance: IOPS, latência e taxa de transferência
- Capacidade: Tamanho, lógico usado, disponível

Você pode visualizar os dados de monitoramento na guia **Visão geral** do menu do grupo de consistência no System Manager ou solicitando-os na API REST. A partir do ONTAP 9.14,1, você pode visualizar métricas de grupo de consistência com a CLI usando o `consistency-group metrics show` comando.

No ONTAP 9.13,1, você só pode recuperar métricas históricas usando a API REST. A partir do ONTAP 9.14,1, métricas históricas também estão disponíveis no Gerenciador de sistemas.

Proteja grupos de consistência

Grupos de consistência oferecem proteção consistente com as aplicações, garantindo a consistência dos dados em vários volumes ou LIFs. Ao criar uma cópia Snapshot de um grupo de consistência, uma "vedação" é estabelecida no grupo de consistência. A cerca inicia uma fila para e/S até que a operação Snapshot seja concluída, garantindo consistência pontual dos dados em todas as entidades do grupo de consistência. A vedação pode causar um pico transitório na latência durante as operações de criação do Snapshot, como uma política de snapshot agendada ou criar um snapshot com o System Manager. Para obter mais informações no contexto da API REST e da CLI, consulte a documentação da API REST do ONTAP e a página de manual da CLI.

Os grupos de consistência oferecem proteção através de:

- Políticas do Snapshot
- Sincronização ativa do SnapMirror
- [mcc] (Começando com ONTAP 9.11,1)
- Assíncrono com SnapMirror (Começando com ONTAP 9.13,1)
- "Recuperação de desastres da SVM" (Começando com ONTAP 9.14,1)

Criar um grupo de consistência não ativa automaticamente a proteção. As políticas de proteção locais e remotas podem ser definidas ao criar ou depois de criar um grupo de consistência.

Para configurar a proteção em um grupo de consistência, "Proteja um grupo de consistência"consulte .

Para utilizar a proteção remota, você deve atender aos requisitos Sincronização ativa do SnapMirrordo .

As relações de sincronização ativa do SnapMirror não podem ser estabelecidas em volumes montados para acesso nas.

Suporte à verificação de vários administradores para grupos de consistência

A partir do ONTAP 9.16,1, você pode usar a verificação multi-admin (MAV) com grupos de consistência para garantir que certas operações, como criar, modificar ou excluir grupos de consistência, possam ser executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis nas configurações existentes.

"Saiba mais"

Grupos de consistência nas configurações do MetroCluster

A partir do ONTAP 9.11,1, é possível provisionar grupos de consistência com novos volumes em um cluster em uma configuração do MetroCluster. Esses volumes são provisionados em agregados espelhados.

Depois que eles forem provisionados, você poderá mover volumes associados a grupos de consistência entre agregados espelhados e sem espelhamento. Portanto, os volumes associados a grupos de consistência podem ser localizados em agregados espelhados, agregados sem espelhamento ou ambos. É possível modificar agregados espelhados que contêm volumes associados a grupos de consistência para se tornarem sem espelhamento. Da mesma forma, você pode modificar agregados sem espelhamento contendo volumes associados a grupos de consistência para habilitar o espelhamento.

Os volumes e as cópias Snapshot associadas a grupos de consistência colocados em agregados espelhados são replicados para o local remoto (local B). O conteúdo dos volumes no local B fornece uma garantia de ordem de gravação para o grupo de consistência, permitindo que você se recupere do local B em caso de desastre. Você pode acessar as cópias Snapshot do grupo de consistência usando o grupo de consistência com a API REST e o Gerenciador de sistema em clusters que executam o ONTAP 9.11,1 ou posterior. A partir do ONTAP 9.14,1, você também pode acessar cópias Snapshot com a CLI do ONTAP.

Se alguns ou todos os volumes associados a um grupo de consistência estiverem localizados em agregados sem espelhamento que não estejam atualmente acessíveis, OBTENHA ou EXCLUA operações no grupo de consistência se comportarem como se os volumes locais ou agregados de hospedagem estivessem offline.

Configurações de grupo de consistência para replicação

Se o local B estiver executando o ONTAP 9.10,1 ou anterior, somente os volumes associados aos grupos de consistência localizados em agregados espelhados serão replicados para o local B. as configurações do grupo de consistência serão replicados apenas para o local B, se ambos os sites estiverem executando o ONTAP 9.11,1 ou posterior. Após o upgrade do local B para o ONTAP 9.11,1, os dados para grupos de consistência no local A que tenham todos os volumes associados colocados em agregados espelhados são replicados para o local B.

> É recomendável manter pelo menos 20% de espaço livre para agregados espelhados para performance e disponibilidade ideais de storage. Embora a recomendação seja de 10% para agregados não espelhados, os 10% adicionais de espaço podem ser usados pelo sistema de arquivos para absorver alterações incrementais. Mudanças incrementais aumentam a utilização de espaço para agregados espelhados devido à arquitetura baseada em Snapshot copy-on-write da ONTAP. O não cumprimento destas práticas recomendadas pode ter um impactos negativo no desempenho.

Considerações sobre a atualização

Ao atualizar para o ONTAP 9.10,1 ou posterior, os grupos de consistência criados com o SnapMirror ative Sync (anteriormente conhecido como SnapMirror Business Continuity) no ONTAP 9.8 e 9.9.1 são atualizados automaticamente e podem ser gerenciados em **armazenamento > grupos de consistência** no Gerenciador de sistemas ou na API REST do ONTAP para obter mais informações sobre a atualização do ONTAP 9.8 ou 9,9.1, "Considerações sobre atualização e reversão da sincronização ativa do SnapMirror"consulte .

As cópias Snapshot criadas na API REST podem ser gerenciadas por meio da interface do Grupo de consistência do System Manager e pelos endpoints da API REST do grupo de consistência. A partir do ONTAP 9.14,1, snapshots de grupo de consistência também podem ser gerenciados com a CLI do ONTAP.

> Cópias snapshot criadas com os comandos ONTAPI `cg-start` e `cg-commit` não são reconhecidas como snapshots de grupo de consistência e, portanto, não podem ser gerenciadas por meio da interface de grupo de consistência do Gerenciador do sistema ou dos pontos de extremidade do grupo de consistência na API REST do ONTAP. A partir do ONTAP 9.14,1, essas cópias Snapshot podem ser espelhadas para o volume de destino se você estiver usando uma política assíncrona do SnapMirror. Para obter mais informações, Configurar o SnapMirror assíncronoconsulte .

Recursos suportados pelo lançamento

	ONTAP 9.16,1	ONTAP 9.15,1	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1	ONTAP 9.10,1
Grupos hierárquicos de consistência	✓	✓	✓	✓	✓	✓	✓
Proteção local com cópias Snapshot	✓	✓	✓	✓	✓	✓	✓
Sincronização ativa do SnapMirror	✓	✓	✓	✓	✓	✓	✓
Suporte à MetroCluster	✓	✓	✓	✓	✓	✓	
Commits de duas fases (somente API REST)	✓	✓	✓	✓	✓	✓	
Tags de aplicativos e componentes	✓	✓	✓	✓	✓		
Grupos de consistência de clones	✓	✓	✓	✓	✓		
Adicionar e remover volumes	✓	✓	✓	✓	✓		
Crie CGS com novos volumes nas	✓	✓	✓	✓	Somente API REST		
Crie CGS com novos namespaces NVMe	✓	✓	✓	✓	Somente API REST		
Mover volumes entre grupos de consistência filho	✓	✓	✓	✓			
Modifique a geometria do grupo de consistência	✓	✓	✓	✓			
Monitorização	✓	✓	✓	✓			
Verificação multi-admin	✓						
Assíncrono SnapMirror (somente grupos de consistência únicos)	✓	✓	✓	✓			
Recuperação de desastres da SVM (somente grupos de consistência únicos)	✓	✓	✓				
Suporte CLI	✓	✓	✓				

Saiba mais sobre grupos de consistência

Informações relacionadas

- "Documentação de automação do ONTAP"
- Sincronização ativa do SnapMirror
- Noções básicas de recuperação de desastres assíncrona do SnapMirror
- "Documentação do MetroCluster"
- "Verificação multi-admin"

Limites do grupo de consistência

Ao Planejar e gerenciar seus grupos de consistência, considere os limites de objetos no escopo do cluster e do grupo de consistência pai ou filho.

Limites impostos

A tabela a seguir captura limites para grupos de consistência. Limites separados se aplicam a grupos de consistência usando a sincronização ativa do SnapMirror. Para obter mais informações, "Limites de sincronização ativa do SnapMirror"consulte .

Limite	Âmbito de aplicação	Mínimo	Máximo
Número de grupos de consistência	Cluster	0	Igual à contagem máxima de volume no cluster*
Número de grupos de consistência pai	Cluster	0	Igual à contagem máxima de volume no cluster
Número de grupos de consistência individual e pai	Cluster	0	Igual à contagem máxima de volume no cluster

Número de volumes em um grupo de consistência	Grupo de consistência único	volume 1	80 volumes
Número de volumes em um grupo de consistência com o SnapMirror assíncrono	Grupo de consistência único	volume 1	• Em ONTAP 9.15,1 e posterior: 80 volumes • Em ONTAP 9.13,1 e 9.14.1: 16 volumes
Número de volumes no filho de um grupo de consistência pai	Grupo de consistência pai	volume 1	80 volumes
Número de volumes em um grupo de consistência filho	Grupo de consistência infantil	volume 1	80 volumes
Número de grupos filhos de consistência em um grupo pai de consistência	Grupo de consistência pai	1 grupo de consistência	5 grupos de consistência
Número de relacionamentos de recuperação de desastres do SVM em que existe um grupo de consistência (disponível a partir do ONTAP 9.14,1)	Cluster	0	32

Um máximo de 50 grupos de consistência habilitados com o SnapMirror assíncrono podem ser hospedados em um cluster.

Limites não aplicados

O agendamento mínimo de cópia Snapshot compatível para grupos de consistência é de 30 minutos. Isso é baseado "Teste para FlexGroups"no , que compartilha a mesma infraestrutura Snapshot que os grupos de consistência.

Configurar um único grupo de consistência

Os grupos de consistência podem ser criados com volumes existentes ou novos LUNs ou volumes (dependendo da versão do ONTAP). Um volume ou LUN só pode ser associado a um grupo de consistência de cada vez.

Sobre esta tarefa

- No ONTAP 9.10,1 a 9.11.1, a modificação dos volumes de membros de um grupo de consistência após a criação não é suportada.

  A partir do ONTAP 9.12,1, você pode modificar os volumes de membros de um grupo de consistência. Para obter mais informações sobre este processo, Modifique um grupo de consistênciaconsulte .

Crie um grupo de consistência com novos LUNs ou volumes

No ONTAP 9.10,1 a 9.12.1, você pode criar um grupo de consistência usando novos LUNs. A partir do ONTAP

9.13,1, o System Manager também dá suporte à criação de um grupo de consistência com novos namespaces NVMe ou novos volumes nas. (Isso também é suportado na API REST do ONTAP começando com ONTAP 9.12,1.)

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar * e, em seguida, selecione o protocolo para o seu objeto de armazenamento.

   No ONTAP 9.10,1 até 9.12.1, a única opção para um novo objeto de armazenamento é **usando novos LUNs**. A partir do ONTAP 9.13,1, o System Manager dá suporte à criação de grupos de consistência com novos namespaces NVMe e novos volumes nas.

3. Nomeie o grupo de consistência. Designar o número de volumes ou LUNs e a capacidade por volume ou LUN.
   a. **Tipo de aplicativo**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de aplicativo. Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se você planeja criar um grupo de consistência com uma política de proteção remota, use **Other**.
   b. Para **novos LUNs**: Selecione o sistema operacional host e o formato LUN. Insira as informações do iniciador do host.
   c. Para **novos volumes nas**: Escolha a opção de exportação apropriada (NFS ou SMB/CIFS) com base na configuração nas do SVM.
   d. Para **novos namespaces NVMe**: Selecione o sistema operacional do host e o subsistema NVMe.
4. Para configurar políticas de proteção, adicione um grupo de consistência filho ou permissões de acesso, selecione **mais opções**.
5. Selecione **Guardar**.
6. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparecerá quando o trabalho for concluído. Se você definir uma política de proteção, saberá que ela foi aplicada quando você vir um escudo verde sob olhar sob a política apropriada, remota ou local.

CLI

A partir do ONTAP 9.14,1, é possível criar um novo grupo de consistência com novos volumes usando a CLI do ONTAP. Os parâmetros específicos dependem se os volumes são SAN, NVMe ou NFS.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Criar um grupo de consistência com volumes NFS

1. Crie o grupo de consistência:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

Crie um grupo de consistência com volumes SAN

1. Crie o grupo de consistência:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

Crie um grupo de consistência com namespaces NVMe

1. Crie o grupo de consistência:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

Depois de terminar

1. Confirme que seu grupo de consistência foi criado usando o `consistency-group show` comando.

Crie um grupo de consistência com volumes existentes

Você pode usar volumes existentes para criar um grupo de consistência.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar* e depois **usando volumes existentes**.
3. Nomeie o grupo de consistência e selecione a VM de armazenamento.
   a. **Tipo de aplicativo**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de aplicativo. Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se o grupo consistência tiver uma relação de sincronização ativa do SnapMirror, você deve usar **Other**.

      Em versões do ONTAP anteriores ao ONTAP 9.15,1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror.

4. Selecione os volumes existentes a incluir. Apenas os volumes que ainda não fazem parte de um grupo de consistência estarão disponíveis para seleção.

   Se estiver criando um grupo de consistência com volumes existentes, o grupo de consistência será compatível com volumes FlexVol. Volumes com ou relacionamentos assíncronos SnapMirror ou SnapMirror podem ser adicionados a grupos de consistência, mas eles não têm reconhecimento de grupo de consistência. Os grupos de consistência não são compatíveis com buckets do S3 ou VMs de storage com relacionamentos SVMDR.

5. Selecione **Guardar**.
6. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparece quando a tarefa ONTAP for concluída. Se você escolheu uma política de proteção, confirme que ela foi corretamente definida selecionando seu grupo de consistência no menu. Se você definir uma política de proteção, sabe que ela foi aplicada quando você vê um escudo verde sob olhar sob a política apropriada, remota ou local.

CLI

A partir do ONTAP 9.14,1, é possível criar um grupo de consistência com volumes existentes usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passos

1. Emita o `consistency-group create` comando. O `-volumes` parâmetro aceita uma lista separada por vírgulas de nomes de volume.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

2. Visualize seu grupo de consistência usando o `consistency-group show` comando.

Próximas etapas

- Proteja um grupo de consistência
- Modifique um grupo de consistência
- Clonar um grupo de consistência

Configurar um grupo hierárquico de consistência

Os grupos hierárquicos de consistência permitem gerenciar grandes cargas de trabalho que abrangem vários volumes, criando um grupo de consistência pai que serve como um guarda-chuva para grupos de consistência filhos.

Os grupos hierárquicos de consistência têm um pai que pode incluir até cinco grupos de consistência individuais. Os grupos hierárquicos de consistência podem oferecer suporte a diferentes políticas de Snapshot locais em grupos de consistência ou volumes individuais. Se você usar uma política de proteção remota, isso se aplicará a todo o grupo hierárquico de consistência (pai e filhos).

Começando com ONTAP 9.13,1, você pode modifique a geometria de seus grupos de consistência e mover volumes entre grupos de consistência filho.

Para obter os limites de objetos em grupos de consistência, Limites de objetos para grupos de consistênciaconsulte .

Crie um grupo hierárquico de consistência com novos LUNs ou volumes

Ao criar um grupo de consistência hierárquica, você pode preenchê-lo com novos LUNs. A partir do ONTAP 9.13,1, você também pode usar novos namespaces NVMe e volumes nas.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar * e, em seguida, selecione o protocolo para o seu objeto de armazenamento.

   No ONTAP 9.10,1 até 9.12.1, a única opção para um novo objeto de armazenamento é **usando novos LUNs**. A partir do ONTAP 9.13,1, o System Manager dá suporte à criação de grupos de consistência com novos namespaces NVMe e novos volumes nas.

3. Nomeie o grupo de consistência. Designar o número de volumes ou LUNs e a capacidade por volume ou LUN.
   a. **Tipo de aplicativo**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de aplicativo. Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se você pretende usar uma política de proteção remota, você deve escolher **outro**.
4. Selecione o sistema operacional host e o formato LUN. Insira as informações do iniciador do host.
   a. Para **novos LUNs**: Selecione o sistema operacional host e o formato LUN. Insira as informações do iniciador do host.
   b. Para **novos volumes nas**: Escolha a opção de exportação apropriada (NFS ou SMB/CIFS) com base na configuração nas do SVM.
   c. Para **novos namespaces NVMe**: Selecione o sistema operacional do host e o subsistema NVMe.
5. Para adicionar um grupo de consistência filho, selecione **mais opções** e depois * Adicionar grupo de consistência filho*.
6. Selecione o nível de performance, o número de LUNs ou volumes e a capacidade por LUN ou volume. Designe as configurações de exportação apropriadas ou as informações do sistema operacional com base no protocolo que você está usando.
7. Opcionalmente, selecione uma política de snapshot local e defina as permissões de acesso.
8. Repita para até cinco grupos de consistência infantil.
9. Selecione **Guardar**.
10. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparecerá quando a tarefa ONTAP for concluída. Se você definir uma política de proteção, observe a política apropriada, remota ou local, que deve exibir um escudo verde com uma marca de seleção nela.

CLI

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Ao criar um grupo de consistência hierárquica na CLI com novos volumes, você deve criar cada grupo de consistência filho individualmente.

Passo

1. Crie o novo grupo de consistência usando o `consistency-group create` comando.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
   -count <number_of_volumes> -size <size>
   ```

2. Quando solicitado pela CLI, confirme que você deseja criar o novo grupo de consistência pai. Introduza `y`.
3. Opcionalmente, repita a etapa 1 para criar mais grupos de consistência filho.

Crie um grupo de consistência hierárquica com volumes existentes

Você pode organizar volumes existentes em um grupo hierárquico de consistência.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione * Adicionar* e depois **usando volumes existentes**.
3. Selecione a VM de armazenamento.
4. Selecione os volumes existentes a incluir. Apenas os volumes que ainda não fazem parte de um grupo de consistência estarão disponíveis para seleção.
5. Para adicionar um grupo de consistência filho, selecione * Adicionar grupo de consistência filho*. Crie os grupos de consistência necessários, que serão nomeados automaticamente.
   a. **Tipo de componente**: Se você estiver usando o ONTAP 9.12,1 ou posterior, selecione um tipo de componente de "dados", "logs" ou "Other". Se nenhum valor for selecionado, o grupo de consistência será atribuído o tipo de **outro** por padrão. Saiba mais sobre a consistência da marcação no Tags de aplicativos e componentes. Se você pretende usar uma política de proteção remota, você deve usar **outro**.
6. Atribua volumes existentes a cada grupo de consistência.
7. Opcionalmente, selecione uma política de instantâneo local.
8. Repita para até cinco grupos de consistência infantil.
9. Selecione **Guardar**.
10. Confirme que o seu grupo de consistência foi criado retornando ao menu principal do grupo de consistência, onde ele aparecerá quando a tarefa ONTAP for concluída. Se você escolheu uma política de proteção, confirme que ela foi corretamente definida selecionando seu grupo de consistência no menu; no tipo de política apropriado, você verá um escudo verde com uma marca de seleção dentro dela.

CLI

A partir do ONTAP 9.14,1, você pode criar um grupo hierárquico de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passos

1. Provisione um novo grupo de consistência pai e atribua volumes a um novo grupo de consistência filho:

```
consistency-group create -vserver <svm_name> -consistency-group
<child_consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volumes <volume_names>
```

2. Digite `y` para confirmar que deseja criar um novo grupo de consistência pai e filho.

Próximas etapas

- Modifique a geometria de um grupo de consistência

- Modifique um grupo de consistência
- Proteja um grupo de consistência

Proteja grupos de consistência

Os grupos de consistência oferecem proteção local e remota facilmente gerenciada para aplicações SAN, nas e NVMe que abrangem vários volumes.

Criar um grupo de consistência não ativa automaticamente a proteção. As políticas de proteção podem ser definidas no momento da criação ou após a criação do seu grupo de consistência. Você pode proteger grupos de consistência usando:

- Cópias Snapshot locais
- SnapMirror ative Sync (referido como SnapMirror Business Continuity em versões do ONTAP anteriores a 9.15.1)
- MetroCluster (início de 9.11.1)
- SnapMirror assíncrono (início de 9.13.1)
- Recuperação assíncrona de desastres do SVM (início de 9.14.1)

Se você estiver utilizando grupos de consistência aninhados, poderá definir políticas de proteção diferentes para os grupos de consistência pai e filho.

Começando com ONTAP 9.11,1, grupos de consistência oferecem Criação de Snapshot do grupo de consistência em duas fases. A operação Snapshot de duas fases executa uma pré-verificação, garantindo que a cópia Snapshot seja capturada com êxito.

A recuperação pode ocorrer para um grupo inteiro de consistência, um único grupo de consistência em uma configuração hierárquica ou para volumes individuais dentro do grupo de consistência. A recuperação pode ser obtida selecionando o grupo de consistência do qual você deseja recuperar, selecionando o tipo de cópia Snapshot e identificando a cópia Snapshot para basear a restauração. Para obter mais informações sobre esse processo, "Restaurar um volume a partir de uma cópia Snapshot anterior"consulte .

Configurar uma política de instantâneo local

Definir uma política de proteção de snapshot local permite criar uma política que abrange todos os volumes em um grupo de consistência.

Sobre esta tarefa

O agendamento mínimo de cópia Snapshot compatível para grupos de consistência é de 30 minutos. Isso é baseado "Teste para FlexGroups"no , que compartilha a mesma infraestrutura Snapshot que os grupos de consistência.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que você criou no menu do grupo de consistência.
3. No canto superior direito da página de visão geral do grupo consistência, selecione **Editar**.
4. Marque a caixa ao lado de **Agendar cópias Snapshot (local)**.
5. Selecione uma política de instantâneos. Para configurar uma nova política personalizada, "Crie uma política de proteção de dados personalizada"consulte .
6. Selecione **Guardar**.
7. Regresse ao menu de visão geral do grupo de consistência. Na coluna à esquerda em **cópias Snapshot (local)**, o status dirá protegido ao lado de .

CLI

A partir do ONTAP 9.14,1, você pode modificar a política de proteção de um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passo

1. Execute o seguinte comando para definir ou modificar a política de proteção:

   Se você estiver modificando a política de proteção de uma consistência filho, será necessário identificar o grupo de consistência pai usando o `-parent-consistency-group` *`parent_consistency_group_name`* parâmetro.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Crie uma cópia Snapshot sob demanda

Se você precisar criar uma cópia Snapshot do seu grupo de consistência fora de uma política normalmente agendada, poderá criar uma sob demanda.

System Manager

Passos

1. Navegue até **armazenamento** > **grupos de consistência**.
2. Selecione o grupo de consistência para o qual você deseja criar uma cópia Snapshot sob demanda.
3. Mude para a guia **cópias Snapshot** e selecione * Adicionar*.
4. Forneça um **Nome** e um **Etiqueta SnapMirror**. No menu suspenso para **consistência**, selecione **consistente aplicação** ou **Crash consistente**.
5. Selecione **Guardar**.

CLI

A partir do ONTAP 9.14,1, você pode criar uma cópia Snapshot sob demanda de um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passo

1. Criar a cópia Snapshot:

   Por padrão, o tipo Snapshot é consistente com falhas. Você pode modificar o tipo de instantâneo com o parâmetro opcional `-type`.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Crie instantâneos de grupo de consistência em duas fases

A partir do ONTAP 9.11,1, os grupos de consistência suportam commits de duas fases para a criação de instantâneo do grupo de consistência (CG), que executam uma pré-verificação antes de confirmar a cópia Snapshot. Esse recurso só está disponível com a API REST do ONTAP.

A criação de Snapshot CG em duas fases só está disponível para a criação do Snapshot, não para provisionar grupos de consistência ou restaurar grupos de consistência.

Um CG Snapshot de duas fases divide o processo de criação de Snapshot em duas fases:

1. Na primeira fase, a API executa pré-verificações e aciona a criação do Snapshot. A primeira fase inclui um parâmetro de tempo limite, designando a quantidade de tempo para a cópia Snapshot ser confirmada com êxito.
2. Se a solicitação na primeira fase for concluída com êxito, você poderá invocar a segunda fase dentro do intervalo designado a partir da primeira fase, comprometendo a cópia Snapshot ao endpoint apropriado.

Antes de começar

- Para usar a criação de Snapshot CG em duas fases, todos os nós do cluster devem estar executando o ONTAP 9.11,1 ou posterior.

- Apenas uma invocação ativa de uma operação Snapshot de grupo de consistência é suportada em uma instância de grupo de consistência de cada vez, seja em uma fase ou em duas fases. A tentativa de invocar uma operação Snapshot enquanto outra está em andamento resulta em uma falha.
- Quando você invoca criação do Snapshot, você pode definir um valor de tempo limite opcional entre 5 e 120 segundos. Se nenhum valor de tempo limite for fornecido, o tempo de operação expira no padrão de 7 segundos. Na API, defina o valor de tempo limite com o `action_timeout` parâmetro. Na CLI, use a `-timeout` bandeira.

Passos

Você pode concluir um snapshot de duas fases com a API REST ou, a partir do ONTAP 9.14,1, a CLI do ONTAP. Esta operação não é suportada no System Manager.

Se você invocar a criação do Snapshot com a API, deverá confirmar a cópia Snapshot com a API. Se você invocar a criação do Snapshot com a CLI, deverá confirmar a cópia Snapshot com a CLI. Os métodos de mistura não são suportados.

CLI

A partir do ONTAP 9.14,1, você pode criar uma cópia Snapshot em duas fases usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passos

1. Inicie o instantâneo:

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Verifique se o instantâneo foi obtido:

   ```
   consistency-group snapshot show
   ```

3. Confirme o snapshot:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Invoque a criação do Snapshot. Envie uma SOLICITAÇÃO POST para o endpoint do grupo de consistência usando o `action=start` parâmetro.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. Se a SOLICITAÇÃO POST for bem-sucedida, a saída inclui um uuuid Snapshot. Usando esse uuid, envie uma SOLICITAÇÃO DE PATCH para confirmar a cópia Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Defina a proteção remota para um grupo de consistência

Os grupos de consistência oferecem proteção remota por meio da sincronização ativa do SnapMirror e, a partir do ONTAP 9.13,1, assíncrono do SnapMirror.

Configure a proteção com a sincronização ativa do SnapMirror

Você pode utilizar a sincronização ativa do SnapMirror para garantir que as cópias Snapshot dos grupos de consistência criados no grupo de consistência sejam copiadas para o destino. Para saber mais sobre a sincronização ativa do SnapMirror ou como configurar a sincronização ativa do SnapMirror usando a CLI, Configurar a proteção para a continuidade dos negóciosconsulte .

Antes de começar

- As relações de sincronização ativa do SnapMirror não podem ser estabelecidas em volumes montados para acesso nas.
- Os rótulos de política no cluster de origem e destino devem corresponder.
- O SnapMirror active Sync não replicará cópias Snapshot por padrão, a menos que uma regra com um rótulo SnapMirror seja adicionada à política predefinida `AutomatedFailOver` e as cópias Snapshot sejam criadas com esse rótulo.

  Para saber mais sobre este processo, "Proteja com a sincronização ativa do SnapMirror"consulte .

- Implantações em cascata Não são compatíveis com a sincronização ativa do SnapMirror.
- Começando com ONTAP 9.13,1, você pode sem interrupções adicione volumes a um grupo de consistência com uma relação de sincronização ativa do SnapMirror. Quaisquer outras alterações em um grupo de consistência exigem que você quebre a relação de sincronização ativa do SnapMirror, modifique o grupo de consistência e, em seguida, restabeleça e ressincronize a relação.

Para configurar a sincronização ativa do SnapMirror com a CLI, Proteja com a sincronização ativa do SnapMirrorconsulte .

Etapas para o System Manager

1. Certifique-se de que encontrou o "Pré-requisitos para usar a sincronização ativa do SnapMirror".
2. Selecione **armazenamento > grupos de consistência**.
3. Selecione o grupo de consistência que você criou no menu do grupo de consistência.
4. No canto superior direito da página de visão geral, selecione **mais** e depois **proteger**.

5. O System Manager preenche automaticamente as informações do lado da fonte. Selecione o cluster e a VM de armazenamento apropriados para o destino. Selecione uma política de proteção. Certifique-se de que **Initialize Relationship** está marcado.
6. Selecione **Guardar**.
7. O grupo de consistência precisa inicializar e sincronizar. Confirme se a sincronização foi concluída com êxito retornando ao menu **Grupo de consistência**. O status **SnapMirror (remoto)** é exibido `Protected` ao lado  de .

Configurar o SnapMirror assíncrono

A partir do ONTAP 9.13,1, você pode configurar a proteção assíncrona do SnapMirror para um único grupo de consistência. A partir do ONTAP 9.14,1, você pode usar o assíncrono SnapMirror para replicar cópias Snapshot granular de volume para o cluster de destino usando o relacionamento de grupo de consistência.

Sobre esta tarefa

Para replicar cópias Snapshot granular de volume, você precisa executar o ONTAP 9.14,1 ou posterior. Para políticas MirrorAndVault e Vault, o rótulo SnapMirror da política de snapshot granular de volume deve corresponder à regra de política SnapMirror do grupo de consistência. Os snapshots granulares em volume cumprem o valor manter da política SnapMirror do grupo de consistência, que é calculada independentemente dos snapshots do grupo de consistência. Por exemplo, se você tiver uma política para manter duas cópias Snapshot no destino, poderá ter duas cópias Snapshot granular de volume e duas cópias Snapshot de grupo de consistência.

Ao ressincronizar a relação do SnapMirror com cópias Snapshot granular de volume, é possível preservar as cópias Snapshot granular de volume com o `-preserve` sinalizador. Cópias Snapshot granular de volume mais recentes que o grupo de consistência as cópias Snapshot são preservadas. Se não houver uma cópia Snapshot de grupo de consistência, nenhuma cópia Snapshot granular de volume poderá ser transferida para a operação ressincronizada.

Antes de começar

- A proteção assíncrona do SnapMirror está disponível apenas para um único grupo de consistência. Não é suportado para grupos hierárquicos de consistência. Para converter um grupo de consistência hierárquica em um único grupo de consistência, modifique a arquitetura do grupo de consistênciaconsulte .
- Os rótulos de política no cluster de origem e destino devem corresponder.
- Você pode sem interrupções adicione volumes a um grupo de consistência com uma relação assíncrona ativa do SnapMirror. Quaisquer outras alterações em um grupo de consistência exigem que você quebre o relacionamento SnapMirror, modifique o grupo de consistência e, em seguida, restabeleça e ressincronize o relacionamento.
- Os grupos de consistência habilitados para proteção com o SnapMirror Asynchronous têm limites diferentes. Para obter mais informações, Limites do grupo de consistênciaconsulte .
- Se você tiver configurado uma relação de proteção assíncrona do SnapMirror para vários volumes individuais, poderá converter esses volumes em um grupo de consistência e reter as cópias Snapshot existentes. Para converter volumes com sucesso:
  - Deve haver uma cópia Snapshot comum dos volumes.
  - Você deve quebrar a relação existente do SnapMirror eadicione os volumes a um único grupo de consistência, em seguida, ressincronizar a relação usando o seguinte fluxo de trabalho.

Passos

1. No cluster de destino, selecione **armazenamento > grupos de consistência**.

2. Selecione o grupo de consistência que você criou no menu do grupo de consistência.
3. No canto superior direito da página de visão geral, selecione **mais** e depois **proteger**.
4. O System Manager preenche automaticamente as informações do lado da fonte. Selecione o cluster e a VM de armazenamento apropriados para o destino. Selecione uma política de proteção. Certifique-se de que **Initialize Relationship** está marcado.

   Ao selecionar uma política assíncrona, você tem a opção de **Substituir programação de transferência**.

   > O cronograma mínimo com suporte (objetivo do ponto de restauração ou RPO) para grupos de consistência com assíncrono SnapMirror é de 30 minutos.

5. Selecione **Guardar**.
6. O grupo de consistência precisa inicializar e sincronizar. Confirme se a sincronização foi concluída com êxito retornando ao menu **Grupo de consistência**. O status **SnapMirror (remoto)** é exibido `Protected` ao lado de .

Configurar a recuperação de desastres da SVM

A partir do ONTAP 9.14,1, Recuperação de desastres da SVM suporta grupos de consistência, permitindo espelhar informações do grupo de consistência da origem para o cluster de destino.

Se você habilitar a recuperação de desastres do SVM em uma SVM que já contenha um grupo de consistência, siga os workflows de configuração do SVM System Managerpara ou o CLI do ONTAP.

Se você estiver adicionando um grupo de consistência a um SVM que esteja em uma relação de recuperação de desastres ativa e saudável da SVM, você precisará atualizar a relação de recuperação de desastres do SVM no cluster de destino. Para obter mais informações, Atualizar uma relação de replicação manualmenteconsulte . Você deve atualizar o relacionamento sempre que expandir o grupo de consistência.

Limitações

- A recuperação de desastres da SVM não dá suporte a grupos de consistência hierárquicos.
- A recuperação de desastre do SVM não dá suporte a grupos de consistência protegidos com o SnapMirror assíncrono. É necessário interromper a relação do SnapMirror antes de configurar a recuperação de desastres da SVM.
- Ambos os clusters devem estar executando o ONTAP 9.14,1 ou posterior.
- As relações de fan-out não são compatíveis com configurações de recuperação de desastres da SVM que contenham grupos de consistência.
- Para outros limites, limites do grupo de consistênciaconsulte .

Visualize relacionamentos

O System Manager visualiza mapas LUN no menu **proteção > relacionamentos**. Quando você seleciona uma relação de origem, o System Manager exibe uma visualização das relações de origem. Ao selecionar um volume, você pode aprofundar esses relacionamentos para ver uma lista dos LUNs contidos e dos relacionamentos do grupo de iniciadores. Essas informações podem ser baixadas como uma pasta de trabalho do Excel a partir da exibição de volume individual; a operação de download é executada em segundo plano.

Informações relacionadas

- "Clonar um grupo de consistência"

- "Configurar cópias Snapshot"
- "Crie políticas de proteção de dados personalizadas"
- "Recuperar de cópias Snapshot"
- "Restaurar um volume a partir de uma cópia Snapshot anterior"
- "Descrição geral da sincronização ativa do SnapMirror"
- "Documentação de automação do ONTAP"
- Noções básicas de recuperação de desastres assíncrona do SnapMirror

Modificar volumes de membros em um grupo de consistência

A partir do ONTAP 9.12,1, é possível modificar um grupo de consistência removendo volumes ou adicionando volumes (expandindo o grupo de consistência). A partir do ONTAP 9.13,1, é possível mover volumes entre grupos de consistência filho se eles compartilharem um pai comum.

Adicione volumes a um grupo de consistência

A partir do ONTAP 9.12,1, você pode adicionar volumes a um grupo de consistência sem interrupções.

Sobre esta tarefa

- Não é possível adicionar volumes associados a outro grupo de consistência.
- Os grupos de consistência são compatíveis com protocolos nas, SAN e NVMe.
- Você pode adicionar até 16 volumes de cada vez a um grupo de consistência se os ajustes estiverem dentro do limites do grupo de consistência.
- A partir do ONTAP 9.13,1, você pode adicionar volumes a um grupo de consistência sem interrupções com uma política de sincronização ativa do SnapMirror ativa ou assíncrona do SnapMirror.
- Quando você adiciona volumes a um grupo de consistência protegido pela sincronização ativa do SnapMirror, o status da relação de sincronização ativa do SnapMirror muda para "expansão" até que o espelhamento e a proteção estejam configurados para o novo volume. Se ocorrer um desastre no cluster primário antes que esse processo seja concluído, o grupo de consistência voltará à sua composição original como parte da operação de failover.
- No ONTAP 9.12,1 e anteriores, _não é possível adicionar volumes a um grupo de consistência em uma relação de sincronização ativa do SnapMirror. Primeiro, você deve excluir a relação de sincronização ativa do SnapMirror, modificar o grupo de consistência e restaurar a proteção com a sincronização ativa do SnapMirror.
- A partir do ONTAP 9.12,1, a API REST do ONTAP suporta a adição de *new* ou volumes existentes a um grupo de consistência. Para obter mais informações sobre a API REST do ONTAP, "Documentação de referência da API REST do ONTAP"consulte .

  A partir do ONTAP 9.13,1, essa funcionalidade é suportada no Gerenciador de sistemas.
- Ao expandir um grupo de consistência, as cópias Snapshot do grupo de consistência capturado antes da modificação serão consideradas parciais. Qualquer operação de restauração com base nessa cópia Snapshot refletirá o grupo de consistência no momento do snapshot.
- Se você estiver usando ONTAP 9.10,1 até 9.11.1, não poderá modificar um grupo de consistência. Para alterar a configuração de um grupo de consistência no ONTAP 9.10,1 ou 9.11.1, você deve excluir o grupo de consistência e criar um novo grupo de consistência com os volumes que deseja incluir.

- A partir do ONTAP 9.14,1, é possível replicar snapshots granular de volume para o cluster de destino usando o SnapMirror assíncrono. Ao expandir um grupo de consistência usando o SnapMirror assíncrono, os snapshots granulares de volume só são replicados depois de expandir o grupo de consistência quando a política SnapMirror é EspelrorAll ou EspelrorAndVault. Somente snapshots granulares em volume mais recentes que o grupo de consistência de linha de base Snapshot são replicados.
- Se você adicionar volumes a um grupo de consistência em uma relação de recuperação de desastres da SVM (compatível a partir de ONTAP 9.14,1), será necessário atualizar a relação de recuperação de desastres da SVM do cluster de destino após a expansão do grupo de consistência. Para obter mais informações, Atualizar uma relação de replicação manualmenteconsulte .

Exemplo 28. Passos

System Manager

A partir do ONTAP 9.12,1, você pode executar esta operação com o Gerenciador do sistema.

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja modificar.
3. Se você estiver modificando um único grupo de consistência, na parte superior do menu **volumes**, selecione **mais** e, em seguida, **expandir** para adicionar um volume.

   Se você estiver modificando um grupo de consistência filho, identifique o grupo de consistência pai que deseja modificar. Selecione o botão **>** para visualizar os grupos de consistência filho e, em seguida, selecione ⋮ ao lado do nome do grupo de consistência filho que deseja modificar. Nesse menu, selecione **expandir**.
4. Selecione até 16 volumes para adicionar ao grupo de consistência.
5. Selecione **Guardar**. Quando a operação for concluída, exiba os volumes recém-adicionados no menu **volumes** do grupo de consistência.

CLI

A partir do ONTAP 9.14,1, é possível adicionar volumes a um grupo de consistência usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Adicionar volumes existentes

1. Emita o seguinte comando. O `-volumes` parâmetro aceita uma lista de volumes separados por vírgulas.

   ⓘ Inclua o parâmetro somente `-parent-consistency-group` se o grupo de consistência estiver em uma relação hierárquica.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Adicione novos volumes

O procedimento para adicionar novos volumes depende do protocolo que está a utilizar.

ⓘ Inclua o parâmetro somente `-parent-consistency-group` se o grupo de consistência estiver em uma relação hierárquica.

- Para adicionar novos volumes sem exportá-los:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  ```

```
child_consistency_group -parent-consistency-group existingParentCg -volume
volume_name -size size
```

- Para adicionar novos volumes NFS:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- Para adicionar novos volumes SAN:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Para adicionar novos namespaces NVMe:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

Remover volumes de um grupo de consistência

Os volumes removidos de um grupo de consistência não são excluídos. Eles permanecem ativos no cluster.

Sobre esta tarefa

- Não é possível remover volumes de um grupo de consistência em uma relação de recuperação de desastres do SnapMirror active Sync ou SVM. Primeiro, você deve excluir a relação de sincronização ativa do SnapMirror para modificar o grupo de consistência e, em seguida, restabelecer a relação.
- Se um grupo de consistência não tiver volumes após a operação de remoção, o grupo de consistência será excluído.
- Quando um volume é removido de um grupo de consistência, os instantâneos existentes do grupo de consistência permanecem, mas são considerados inválidos. Os instantâneos existentes não podem ser usados para restaurar o conteúdo do grupo de consistência. Snapshots granulares em volume permanecem válidos.
- Se você excluir um volume do cluster, ele será removido automaticamente do grupo de consistência.
- Para alterar a configuração de um grupo de consistência no ONTAP 9.10,1 ou 9.11.1, você deve excluir o grupo de consistência e criar um novo grupo de consistência com os volumes de membros desejados.
- A exclusão de um volume do cluster removerá automaticamente o grupo de consistência.

System Manager

A partir do ONTAP 9.12,1, você pode executar esta operação com o Gerenciador do sistema.

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência único ou filho que deseja modificar.
3. No menu **volumes**, marque as caixas de seleção ao lado dos volumes individuais que deseja remover do grupo consistência.
4. Selecione **Remover volumes do grupo de consistência**.
5. Confirme se você entende que a remoção dos volumes fará com que todas as cópias Snapshot do grupo de consistência se tornem inválidas e selecione **Remover**.

CLI

A partir do ONTAP 9.14,1, você pode remover volumes de um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Passo

1. Remova os volumes. O `-volumes` parâmetro aceita uma lista de volumes separados por vírgulas.

   Inclua o parâmetro somente `-parent-consistency-group` se o grupo de consistência estiver em uma relação hierárquica.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Mover volumes entre grupos de consistência

A partir do ONTAP 9.13,1, é possível mover volumes entre grupos de consistência filho que compartilham um pai.

Sobre esta tarefa

- Você só pode mover volumes entre grupos de consistência aninhados no mesmo grupo de consistência pai.
- Os instantâneos de grupos de consistência existentes tornam-se inválidos e não são mais acessíveis como instantâneos de grupos de consistência. Instantâneos de volume individuais permanecem válidos.
- As cópias snapshot do grupo de consistência pai permanecem válidas.
- Se você mover todos os volumes para fora de um grupo de consistência filho, esse grupo de consistência será excluído.
- As modificações a um grupo de consistência devem respeitar limites do grupo de consistênciao .

System Manager

A partir do ONTAP 9.12,1, você pode executar esta operação com o Gerenciador do sistema.

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai que contém os volumes que deseja mover. Encontre o grupo de consistência filho e expanda o menu **volumes**. Selecione os volumes que pretende mover.
3. Selecione **mover**.
4. Escolha se deseja mover os volumes para um novo grupo de consistência ou um grupo existente.
   a. Para mover para um grupo de consistência existente, selecione **grupo de consistência filho existente** e escolha o nome do grupo de consistência no menu suspenso.
   b. Para mover para um novo grupo de consistência, selecione **novo grupo de consistência filho**. Insira um nome para o novo grupo de consistência filho e selecione um tipo de componente.
5. Selecione **mover**.

CLI

A partir do ONTAP 9.14,1, é possível mover volumes entre grupos de consistência usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Mover volumes para um novo grupo de consistência filho

1. O comando a seguir cria um novo grupo de consistência filho que contém os volumes designados.

   Ao criar o novo grupo de consistência, você designará novas políticas de snapshot, QoS e disposição em camadas.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Mover volumes para um grupo de consistência filho existente

1. Reatribuir os volumes. O `-volumes` parâmetro aceita uma lista separada por vírgulas de nomes de volume.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Informações relacionadas

- Limites do grupo de consistência
- Clonar um grupo de consistência

Modifique a geometria do grupo de consistência

A partir do ONTAP 9.13,1, você pode modificar a geometria de um grupo de consistência. Modificar a geometria de um grupo de consistência permite alterar a configuração de grupos de consistência pai ou filho sem interromper as operações de e/S em andamento.

A modificação da geometria do grupo de consistência tem impacto nas cópias Snapshot existentes do grupo de consistência. Para obter detalhes, consulte a modificação específica da geometria que deseja executar.

> Não é possível modificar a geometria de um grupo de consistência configurado com uma política de proteção remota. Você deve primeiro quebrar a relação de proteção, modificar a geometria e restaurar a proteção remota.

Adicione um novo grupo de consistência filho

A partir do ONTAP 9.13,1, você pode adicionar um novo grupo de consistência filho a um grupo de consistência pai existente.

Sobre esta tarefa

- Um grupo de consistência pai pode conter no máximo cinco grupos filhos. limites do grupo de consistênciaConsulte para obter outros limites.
- Não é possível adicionar um grupo de consistência filho a um único grupo de consistência. Você deve primeiro [promover] o grupo de consistência, então você pode adicionar um grupo de consistência filho.
- Cópias Snapshot existentes do grupo de consistência capturado antes da operação de expansão serão consideradas parciais. Qualquer operação de restauração baseada nessa cópia Snapshot refletirá o grupo de consistência no momento da cópia Snapshot.

Exemplo 29. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Adicione um novo grupo de consistência filho

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai ao qual deseja adicionar um grupo de consistência filho.
3. Ao lado do nome do grupo de consistência pai, selecione **More** (mais) e depois **Add new child consistency group (Adicionar novo grupo de consistência filho)**.
4. Introduza um nome para o seu grupo de consistência.
5. Escolha se deseja adicionar volumes novos ou existentes.
   a. Se você estiver adicionando volumes existentes, selecione **volumes existentes** e escolha os volumes no menu suspenso.
   b. Se você estiver adicionando novos volumes, selecione **novos volumes** e designe o número de volumes e seu tamanho.
6. Selecione **Adicionar**.

CLI

A partir do ONTAP 9.14,1, você pode adicionar um grupo de consistência filho usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Adicione um grupo de consistência filho com novos volumes

1. Crie o novo grupo de consistência. Forneça valores para o nome do grupo de consistência, prefixo de volume, número de volumes, tamanho do volume, serviço de storage e nome da política de exportação:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Adicione um grupo de consistência filho com volumes existentes

1. Crie o novo grupo de consistência. O `volumes` parâmetro aceita uma lista separada por vírgulas de nomes de volume.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Separe um grupo de consistência infantil

A partir do ONTAP 9.13,1, você pode remover um grupo de consistência filho de seu pai, convertendo-o em um grupo de consistência individual.

Sobre esta tarefa

- Separar um grupo de consistência filho faz com que as cópias Snapshot do grupo de consistência pai se tornem inválidas e inacessíveis. As cópias Snapshot granular de volume permanecem válidas.
- As cópias Snapshot existentes do grupo de consistência individual permanecem válidas.
- Esta operação falhará se houver um único grupo de consistência existente que tenha o mesmo nome do grupo de consistência filho que você pretende separar. Se você encontrar este cenário, você deve renomear o grupo de consistência quando você o desanexar.

Exemplo 30. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Separe um grupo de consistência infantil

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai que contém o filho que você deseja desanexar.
3. Ao lado do grupo de consistência filho que você deseja desanexar, selecione **More** (mais) e depois **Detach from parent** (Desanexar do pai).
4. Opcionalmente, renomeie o grupo de consistência e selecione um tipo de aplicativo.
5. Selecione **Desanexar**.

CLI

A partir do ONTAP 9.14,1, você pode desanexar um grupo de consistência filho usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Separe um grupo de consistência infantil

1. Separe o grupo de consistência. Opcionalmente, renomeie o grupo de consistência destacada com o `-new-name` parâmetro.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Mover um único grupo de consistência existente em um grupo de consistência pai

A partir do ONTAP 9.13,1, você pode converter um único grupo de consistência existente para um grupo de consistência filho. Você pode mover o grupo de consistência em um grupo de consistência pai existente ou criar um novo grupo de consistência pai durante a operação mover.

Sobre esta tarefa

- O grupo de consistência pai deve ter quatro ou menos filhos. Um grupo de consistência pai pode conter no máximo cinco grupos filhos. limites do grupo de consistênciaConsulte para obter outros limites.
- Cópias Snapshot existentes do grupo de consistência *pai* capturadas antes dessa operação são consideradas parciais. Qualquer operação de restauração baseada em uma dessas cópias Snapshot reflete o grupo de consistência no momento da cópia Snapshot.
- As cópias Snapshot do grupo de consistência único permanecem válidas.

Exemplo 31. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Mover um único grupo de consistência existente em um grupo de consistência pai

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja converter.
3. Selecione **More** (mais) e, em seguida, **mover para o grupo de consistência diferente**.
4. Opcionalmente, insira um novo nome para o grupo de consistência e selecione um tipo de componente. Por padrão, o tipo de componente será outro.
5. Escolha se deseja migrar para um grupo de consistência pai existente ou criar um novo grupo de consistência pai:
   a. Para migrar para um grupo de consistência pai existente, selecione **grupo de consistência existente** e escolha o grupo de consistência no menu suspenso.
   b. Para criar um novo grupo de consistência pai, selecione **novo grupo de consistência** e, em seguida, forneça um nome para o novo grupo de consistência.
6. Selecione **mover**.

CLI

A partir do ONTAP 9.14,1, você pode mover um único grupo de consistência em um grupo de consistência pai usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Mover um grupo de consistência em um novo grupo de consistência pai

1. Crie o novo grupo de consistência pai. O `-consistency-groups` parâmetro migrará qualquer grupo de consistência existente para o novo pai.

   ```
   consistency-group attach -vserver svm_name -consistency-group
   parent_consistency_group -consistency-groups child_consistency_group
   ```

Mover um grupo de consistência em um grupo de consistência existente

1. Mover o grupo de consistência:

   ```
   consistency-group add -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   ```

Promover um grupo de consistência infantil

A partir do ONTAP 9.13,1, você pode promover um único grupo de consistência para um grupo de consistência pai. Quando você promove o grupo de consistência único para um pai, você também cria um novo grupo de consistência filho que herda todos os volumes no grupo de consistência original e único.

Sobre esta tarefa

- Se você quiser converter um grupo de consistência filho para um grupo de consistência pai, primeiro [detach] o grupo de consistência filho, siga este procedimento.
- As cópias Snapshot existentes do grupo de consistência permanecem válidas depois que você promover o grupo de consistência.

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Promover um grupo de consistência infantil

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja promover.
3. Selecione **mais** e depois **promover para o grupo de consistência pai**.
4. Digite um **Nome** e selecione um **tipo de componente** para o grupo de consistência filho.
5. Selecione **promover**.

CLI

A partir do ONTAP 9.14,1, você pode mover um único grupo de consistência em um grupo de consistência pai usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Promover um grupo de consistência infantil

1. Promover o grupo de consistência. Este comando criará um grupo de consistência pai e um filho.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

Demote um pai para um único grupo de consistência

A partir do ONTAP 9.13,1, você pode rebaixar um grupo de consistência pai para um único grupo de consistência. A rebaixamento do pai achata a hierarquia do grupo de consistência, removendo todos os grupos de consistência filho associados. Todos os volumes no grupo consistência permanecerão sob o novo grupo de consistência única.

Sobre esta tarefa

- As cópias Snapshot existentes do grupo de consistência *pai* permanecem válidas depois de rebaixá-lo para uma única consistência. Cópias Snapshot existentes de qualquer um dos grupos de consistência *filho* associados desse pai se tornam inválidas ao serem rebaixadas. As cópias Snapshot de volume individual dentro do grupo de consistência filho continuam acessíveis como cópias Snapshot granular de volume.

Exemplo 32. Passos

System Manager

A partir do ONTAP 9.13,1, você pode executar esta operação com o Gerenciador do sistema.

Demote um grupo de consistência

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência pai que deseja rebaixar.
3. Selecione **mais** e depois **demote para um único grupo de consistência**.
4. Um aviso irá informá-lo de que todos os grupos de consistência filho associados serão eliminados e os seus volumes serão movidos para o novo grupo de consistência único. Selecione **demote** para confirmar que compreende o impactos.

CLI

A partir do ONTAP 9.14,1, você pode rebaixar um grupo de consistência usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Demote um grupo de consistência

1. Demote o grupo de consistência. Use o parâmetro opcional `-new-name` para renomear o grupo de consistência.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Modificar tags de aplicativo e componente

A partir do ONTAP 9.12,1, os grupos de consistência suportam a marcação de componentes e aplicativos. Tags de aplicativo e componente são uma ferramenta de gerenciamento, permitindo filtrar e identificar diferentes cargas de trabalho em seus grupos de consistência.

Sobre esta tarefa

Grupos de consistência oferecem dois tipos de tags:

- **Etiquetas de aplicação**: Aplicam-se a grupos de consistência individuais e pai. As tags de aplicação fornecem rotulagem para workloads como MongoDB, Oracle ou SQL Server. A tag padrão do aplicativo para grupos de consistência é outra.
- **Tags de componente**: Crianças em grupos de consistência hierárquica têm tags de componente em vez de tags de aplicativo. As opções para tags de componentes são "dados", "logs" ou "outros". O valor padrão é outro.

Você pode aplicar tags ao criar grupos de consistência ou após os grupos de consistência terem sido criados.

Se o grupo de consistência tiver uma relação de sincronização ativa do SnapMirror, você deve usar **Other** como a tag de aplicativo ou componente.

Passos

A partir do ONTAP 9.12,1, você pode modificar tags de aplicativos e componentes usando o Gerenciador de sistema. A partir do ONTAP 9.14,1, você pode modificar as tags de aplicativo e componente usando a CLI do ONTAP.

System Manager

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência cuja tag você deseja modificar. Selecione o ⋮ ao lado do nome do grupo de consistência e depois **Editar**.
3. No menu suspenso, escolha a aplicação ou a etiqueta de componente apropriada.
4. Selecione **Guardar**.

CLI

A partir do ONTAP 9.14,1, você pode modificar a tag de aplicativo ou componente de um grupo de consistência existente usando a CLI do ONTAP.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Modifique a etiqueta da aplicação

1. As etiquetas de aplicação aceitam um número limitado de strings predefinidas. Para ver a lista aceita de strings, execute o seguinte comando:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Escolha a cadeia de carateres apropriada da saída, o grupo modificar a consistência:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Modifique a etiqueta do componente

1. Modificar o tipo de componente. O tipo de componente pode ser dados, logs ou outro. Se você estiver usando a sincronização ativa do SnapMirror, ela deve ser "outra".
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Clonar um grupo de consistência

A partir do ONTAP 9.12,1, você pode clonar um grupo de consistência para criar uma cópia de um grupo de consistência e seu conteúdo. Clonar um grupo de consistência cria uma cópia da configuração do grupo de consistência, seus metadados, como tipo de aplicação, e todos os volumes e seu conteúdo, como arquivos, diretórios, LUNs ou

namespaces NVMe.

Sobre esta tarefa

Ao clonar um grupo de consistência, é possível cloná-lo com a configuração atual, mas com conteúdo de volume tal como ele está ou baseado em um grupo de consistência Snapshot existente.

Clonar um grupo de consistência é compatível apenas para todo o grupo de consistência. Você não pode clonar um grupo de consistência filho individual em uma relação hierárquica: Somente a configuração completa do grupo de consistência pode ser clonada.

Ao clonar um grupo de consistência, os seguintes componentes não são clonados:

- IGroups
- Mapas LUN
- Subsistemas NVMe
- Mapas de subsistema de namespace NVMe

Antes de começar

- Ao clonar um grupo de consistência, o ONTAP não criará compartilhamentos SMB para os volumes clonados se um nome de compartilhamento não for especificado. * Grupos de consistência clonados não são montados se um caminho de junção não for especificado.
- Se você tentar clonar um grupo de consistência com base em um instantâneo que não reflita os volumes constituintes atuais do grupo de consistência, a operação falhará.
- Depois de clonar um grupo de consistência, você precisa executar a operação de mapeamento apropriada.

  Mapeie grupos para vários LUNsConsulte ou Mapear um namespace NVMe para um subsistema para obter mais informações.

- Clonar um grupo de consistência não é compatível para um grupo de consistência em uma relação de sincronização ativa do SnapMirror ou com quaisquer volumes DP associados.

System Manager

Passos

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja clonar no menu **Grupo de consistência**.
3. No canto superior direito da página de visão geral do grupo consistência, selecione **Clone**.
4. Insira um nome para o novo grupo de consistência clonada ou aceite o nome padrão.
   a. Selecione se deseja ativar "**Provisionamento fino**"o .
   b. Escolha **Split Clone** se você quiser dissociar o grupo de consistência de sua origem e alocar espaço em disco adicional para o grupo de consistência clonada.
5. Para clonar o grupo de consistência em seu estado atual, escolha **Adicionar uma nova cópia Snapshot**.

   Para clonar o grupo de consistência com base em um snapshot, escolha **usar uma cópia Snapshot existente**. Selecionar esta opção irá abrir um novo submenu. Escolha o Snapshot que você deseja usar como base para a operação de clone.
6. Selecione **Clone**.
7. Retorne ao menu **Grupo de consistência** para confirmar que seu grupo de consistência foi clonado.

CLI

A partir do ONTAP 9.14,1, você pode clonar um grupo de consistência usando a CLI com credenciais de administrador do cluster.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Clonar um grupo de consistência

1. O `consistency-group clone create` comando clona o grupo de consistência em seu status de ponto no tempo atual. Para basear a operação de clone em um Snapshot, inclua o `-source -snapshot` parâmetro.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

Próximas etapas

- Mapeie grupos para vários LUNs
- Mapear um namespace NVMe para um subsistema

Excluir um grupo de consistência

Se você decidir que não precisa mais de um grupo de consistência, você pode excluí-lo.

Sobre esta tarefa

- A exclusão de um grupo de consistência exclui a instância do grupo de consistência e *não* afeta os volumes constituintes ou LUNs. A exclusão de um grupo de consistência não resulta na exclusão dos instantâneos presentes em cada volume, mas eles não estarão mais acessíveis como instantâneos de grupo de consistência. No entanto, os snapshots podem continuar sendo gerenciados como snapshots granulares de volume comuns.
- O ONTAP exclui automaticamente um grupo de consistência se todos os volumes no grupo de consistência forem excluídos.
- A exclusão de um grupo de consistência pai resulta na exclusão de todos os grupos de consistência filho associados.
- Se você estiver usando uma versão do ONTAP entre 9.10.1 e 9.12.0, os volumes só poderão ser removidos de um grupo de consistência se o volume em si for excluído, caso em que o volume é removido automaticamente do grupo de consistência. A partir do ONTAP 9.12,1, você pode remover volumes de um grupo de consistência sem excluir o grupo de consistência. Para obter mais informações sobre este processo, Modifique um grupo de consistênciaconsulte .

Exemplo 33. Passos

System Manager

1. Selecione **armazenamento > grupos de consistência**.
2. Selecione o grupo de consistência que deseja excluir.
3. Ao lado do nome do grupo consistência, selecione **Excluir**.

CLI

A partir do ONTAP 9.14,1, você pode excluir um grupo de consistência usando a CLI.

Antes de começar

- Você deve estar no nível de privilégio de administrador para executar esta tarefa.
- No ONTAP 9.14,1, você deve ser um administrador de cluster ou SVM para executar essa tarefa. A partir do ONTAP 9.15,1, qualquer utilizador no nível de privilégios de administrador pode executar esta tarefa.

Excluir um grupo de consistência

1. Excluir o grupo de consistência:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

Sincronização ativa do SnapMirror

Introdução

Descrição geral da sincronização ativa do SnapMirror

O SnapMirror ative Sync (também conhecido como SnapMirror Business Continuity *[SM-BC]*) permite que os serviços de negócios continuem operando mesmo com uma falha completa do local, dando suporte ao failover de aplicações de forma transparente

usando uma cópia secundária. Não há necessidade de intervenção manual ou script personalizado para acionar um failover com a sincronização ativa do SnapMirror.

Disponível a partir do ONTAP 9.9,1, a sincronização ativa do SnapMirror é compatível com clusters AFF, clusters All-Flash SAN Array (ASA) e C-Series (AFF ou ASA). Os clusters primário e secundário devem ser do mesmo tipo: ASA ou AFF. A sincronização ativa do SnapMirror protege aplicações com LUNs iSCSI ou FCP.

A partir do ONTAP 9.15,1, o SnapMirror active Sync oferece suporte a um funcionalidade ativo-ativo simétrica, habilitando operações de e/S de leitura e gravação de ambas as cópias de um LUN protegido com replicação síncrona bidirecional, permitindo que ambas as cópias do LUN forneçam operações de e/S localmente. Antes do ONTAP 9.15,1, a sincronização ativa do SnapMirror suporta apenas configurações ativas/ativas assimétricas, nas quais os dados no local secundário são aumentados para um LUN.

A partir de julho de 2024, o conteúdo de relatórios técnicos publicados anteriormente como PDFs foi integrado à documentação do produto ONTAP. A documentação de sincronização ativa do ONTAP SnapMirror agora inclui conteúdo de *TR-4878: SnapMirror active Sync*.

Benefícios

O SnapMirror ative Sync oferece os seguintes benefícios:

- Disponibilidade contínua para aplicações essenciais aos negócios.
- Capacidade de hospedar aplicações críticas alternadamente de locais primários e secundários.
- Gerenciamento simplificado de aplicações usando grupos de consistência para consistência dependente da ordem de gravação.
- Capacidade de testar failover em cada aplicação.
- Criação instantânea de clones espelhados sem afetar a disponibilidade da aplicação.
- Capacidade de implantar workloads protegidos e não protegidos no mesmo cluster do ONTAP.
- A identidade de LUN permanece a mesma, então o aplicativo as vê como um dispositivo virtual compartilhado.
- Capacidade de reutilizar clusters secundários com flexibilidade para criar clones instantâneos para uso da aplicação para fins de desenvolvimento/teste, UAT ou geração de relatórios, sem impactar a performance ou a disponibilidade da aplicação.

O SnapMirror active Sync permite que você proteja LUNs de dados, o que permite o failover de aplicações de forma transparente, para fins de continuidade dos negócios em caso de desastre. Para obter mais informações, "Casos de uso"consulte .

Conceitos-chave

A sincronização ativa do SnapMirror utiliza grupos de consistência e o Mediador ONTAP para garantir que seus dados sejam replicados e atendidos, mesmo em caso de desastre. Ao Planejar sua implantação de sincronização ativa do SnapMirror, é importante entender os conceitos essenciais do SnapMirror ative Sync e sua arquitetura.

Assimetria e simetria

O SnapMirror ative Sync suporta soluções ativas-ativas assimétricas e, a partir do ONTAP 9.15,1, simétricas. Essas opções referem-se a como os hosts acessam caminhos de armazenamento e gravam dados. Em uma configuração assimétrica, os dados no local secundário são aumentados para um LUN. Em uma configuração ativo-ativo simétrica, ambos os locais podem acessar o storage local para e/S ativa

O ativo-ativo simétrico é otimizado para aplicativos em cluster, incluindo VMware vMSC, cluster de failover do Windows com SQL e Oracle RAC.

Para obter mais informações, Arquitetura de sincronização ativa do SnapMirrorconsulte .

Grupo de consistência

A "grupo de consistência" é uma coleção de volumes do FlexVol que garante consistência para o workload da aplicação que precisa ser protegido para manter a continuidade dos negócios.

O objetivo de um grupo de consistência é tirar imagens instantâneas simultâneas de vários volumes, garantindo assim cópias consistentes com falhas de uma coleção de volumes em um momento. Um grupo de consistência garante que todos os volumes de um conjunto de dados sejam silenciados e, em seguida, encaixados exatamente no mesmo ponto no tempo. Isso fornece um ponto de restauração consistente com dados nos volumes que dão suporte ao conjunto de dados. Um grupo de consistência mantém, assim, consistência dependente da ordem de gravação. Se você decidir proteger aplicativos para a continuidade dos negócios, o grupo de volumes correspondentes a esse aplicativo deve ser adicionado a um grupo de consistência para que um relacionamento de proteção de dados seja estabelecido entre uma origem e um grupo de consistência de destino. A consistência de origem e destino deve conter o mesmo número e tipo de volumes.

Constituinte

Um volume individual ou LUN que faz parte do grupo de consistência protegido na relação de sincronização ativa do SnapMirror.

ONTAP Mediador

O "ONTAP Mediador" recebe informações de integridade sobre nós e clusters ONTAP peered, orquestrando entre os dois e determinando se cada nó/cluster está íntegro e em execução. O Mediador ONTAP fornece as informações de saúde sobre:

- Clusters peer ONTAP
- Nós de cluster de peer ONTAP
- Grupos de consistência (que definem as unidades de failover em uma relação de sincronização ativa do SnapMirror); para cada grupo de consistência, as seguintes informações são fornecidas:
  - Estado de replicação: Não inicializado, em Sincronizar ou fora de Sincronizar
  - Qual cluster hospeda a cópia primária
  - Contexto de operação (usado para failover planejado)

Com essas informações de integridade do ONTAP Mediator, os clusters podem diferenciar entre tipos distintos de falhas e determinar se devem executar um failover automatizado. O Mediador ONTAP é uma das três partes no quorum de sincronização ativa do SnapMirror, juntamente com os clusters do ONTAP (primário e secundário). Para chegar a um consenso, pelo menos duas partes no quórum devem concordar com uma determinada operação.

> A partir do ONTAP 9.15,1, o Gerenciador do sistema exibe o status da relação de sincronização ativa do SnapMirror de qualquer cluster. Você também pode monitorar o status do Mediador ONTAP de qualquer cluster no Gerenciador de sistema. Em versões anteriores do ONTAP, o Gerenciador de sistema exibe o status das relações de sincronização ativa do SnapMirror a partir do cluster de origem.

Failover planejado

Uma operação manual para alterar as funções das cópias em uma relação de sincronização ativa do

SnapMirror. Os locais primários se tornam secundários, e o secundário se torna o primário.

Viés primário e primário

A sincronização ativa do SnapMirror usa um princípio primário que dá preferência à cópia primária para servir e/S no caso de uma partição de rede.

Primary-bias é uma implementação de quórum especial que melhora a disponibilidade de um conjunto de dados protegido por sincronização ativa do SnapMirror. Se a cópia primária estiver disponível, o viés primário entrará em vigor quando o Mediador ONTAP não estiver acessível a partir de ambos os clusters.

Primary-first e Primary bias são suportadas na sincronização ativa do SnapMirror a partir do ONTAP 9.15,1. As cópias primárias são designadas no System Manager e são enviadas com a API REST e CLI.

Failover não planejado automático (AUFO)

Uma operação automática para executar um failover para a cópia espelhada. A operação requer a assistência do Mediador ONTAP para detetar que a cópia primária não está disponível.

Fora de sincronização (OOS)

Quando a e/S do aplicativo não estiver replicando para o sistema de storage secundário, ela será reportada como **fora de sincronia**. Um status fora de sincronia significa que os volumes secundários não são sincronizados com o primário (origem) e que a replicação do SnapMirror não está ocorrendo.

Se o estado do espelho for `Snapmirrored`, isso indica uma falha ou falha de transferência devido a uma operação não suportada.

A sincronização ativa do SnapMirror suporta ressincronização automática, permitindo que as cópias voltem a um estado InSync.

A partir do ONTAP 9.15,1, a sincronização ativa do SnapMirror suporta "reconfiguração automática em configurações de fan-out".

Configuração uniforme e não uniforme

- **O acesso uniforme ao host** significa que os hosts de ambos os locais estão conetados a todos os caminhos para os clusters de armazenamento em ambos os locais. Os caminhos entre os locais são estendidos ao longo da distância.
- **Acesso não uniforme ao host** significa que os hosts em cada local são conetados apenas ao cluster no mesmo local. Caminhos entre locais e caminhos esticados não estão conetados.

> O acesso uniforme de host é compatível com qualquer implantação de sincronização ativa do SnapMirror. O acesso de host não uniforme só é compatível com implantações ativas/ativas simétricas.

RPO zero

RPO significa objetivo do ponto de restauração, que é a quantidade de perda de dados considerada aceitável durante um determinado período de tempo. Zero RPO significa que nenhuma perda de dados é aceitável.

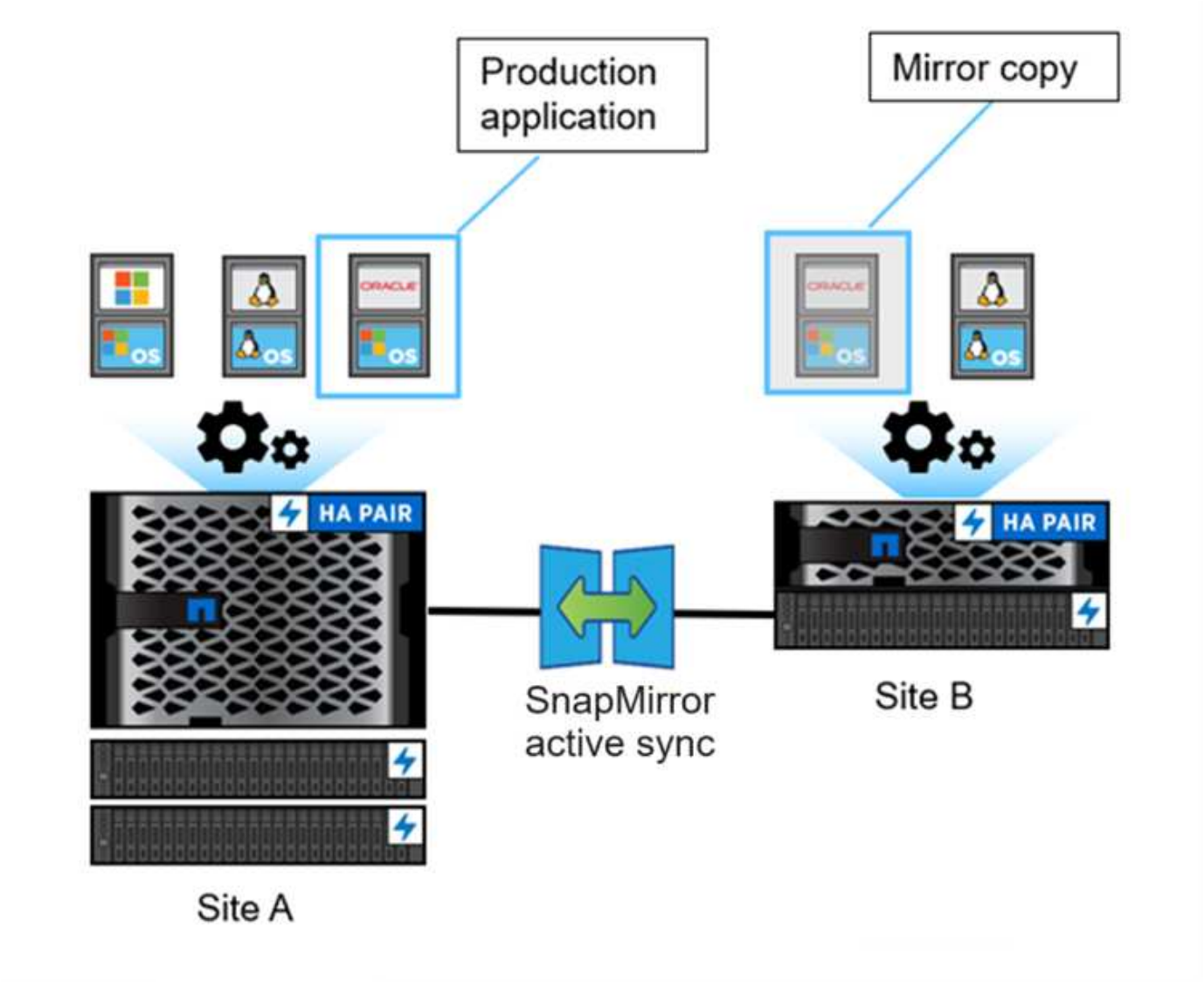
Rto zero

Rto representa o objetivo de tempo de recuperação, que é o tempo que é considerado aceitável para um aplicativo retornar às operações normais sem interrupções, após uma interrupção, falha ou outro evento de perda de dados. Zero rto significa que nenhuma quantidade de tempo de inatividade é aceitável.

Arquitetura de sincronização ativa do SnapMirror

A arquitetura de sincronização ativa do SnapMirror permite workloads ativos nos dois clusters, onde workloads primários podem ser atendidos simultaneamente a partir de ambos os clusters. Os regulamentos para instituições financeiras em alguns países exigem que as empresas sejam periodicamente reparáveis a partir de seus data centers secundários também, chamados de implantações de "Tick-Tock", que o SnapMirror ative Sync permite.

A relação de proteção de dados que protege para manter a continuidade dos negócios é criada entre o sistema de storage de origem e o sistema de storage de destino, adicionando LUNs específicas da aplicação de diferentes volumes em uma máquina virtual de storage (SVM) ao grupo de consistência. Em operações normais, a aplicação empresarial grava no grupo de consistência principal, o que replica de forma síncrona essa e/S para o grupo de consistência espelhada.



Embora existam duas cópias separadas dos dados na relação de proteção de dados, como a sincronização ativa do SnapMirror mantém a mesma identidade de LUN, o host do aplicativo vê isso como um dispositivo virtual compartilhado com vários caminhos, enquanto apenas uma cópia LUN está sendo gravada por vez. Quando uma falha torna o sistema de armazenamento primário offline, o ONTAP deteta essa falha e usa o Mediador para reconfirmação; se nem o ONTAP nem o Mediador forem capazes de fazer ping no local

principal, o ONTAP executará a operação de failover automático. Esse processo resulta em falha apenas de uma aplicação específica sem a necessidade de intervenção manual ou script que anteriormente era necessário para fins de failover.

Outros pontos a considerar:

- São suportados volumes não espelhados que existem fora da proteção para a continuidade dos negócios.
- Somente uma outra relação assíncrona do SnapMirror é suportada para volumes protegidos para continuidade dos negócios.
- Topologias em cascata não são suportadas com proteção para a continuidade dos negócios.

ONTAP Mediador

O ONTAP Mediator é instalado em um terceiro domínio de falha, distinto dos dois clusters ONTAP. Seu papel principal é atuar como uma testemunha passiva das cópias de sincronização ativa do SnapMirror. No caso de uma partição de rede ou indisponibilidade de uma cópia, o SnapMirror SnapMirror ative Sync usa o Mediator para determinar qual cópia continua a servir e/S, enquanto descontinua a e/S na outra cópia. Existem três componentes principais nesta configuração:

- Cluster ONTAP primário que hospeda o CG primário de sincronização ativa do SnapMirror
- Cluster ONTAP secundário que hospeda o CG espelhado
- ONTAP Mediador

O Mediador ONTAP desempenha um papel crucial nas configurações de sincronização ativa do SnapMirror como testemunha de quórum passivo, garantindo a manutenção do quórum e facilitando o acesso aos dados durante falhas. Ele atua como um proxy ping para controladores para determinar a vivacidade dos controladores peer. Embora o Mediator não acione ativamente as operações de comutação, ele fornece uma função vital, permitindo que o nó sobrevivente verifique o status de seu parceiro durante problemas de comunicação de rede. Em seu papel como testemunha de quórum, o Mediador ONTAP fornece um caminho alternativo (servindo efetivamente como proxy) para o cluster de pares.

Além disso, permite que os clusters obtenham essas informações como parte do processo de quórum. Ele utiliza o LIF de gerenciamento de nós e o LIF de gerenciamento de clusters para fins de comunicação. Ele estabelece conexões redundantes através de vários caminhos para diferenciar entre falha do local e falha do InterSwitch Link (ISL). Quando um cluster perde a conexão com o software Mediador ONTAP e todos os seus nós devido a um evento, ele é considerado não alcançável. Isso aciona um alerta e permite o failover automatizado para o Mirror Consistency Group (CG) no local secundário, garantindo e/S ininterrupto para o cliente. O caminho dos dados de replicação depende de um mecanismo de heartbeat, e se uma falha de rede ou evento persistir além de um determinado período, pode resultar em falhas de heartbeat, fazendo com que a relação fique fora de sincronia. No entanto, a presença de caminhos redundantes, como failover de LIF para outra porta, pode sustentar o batimento cardíaco e evitar tais interrupções.

Para resumir, o Mediador ONTAP é usado para os seguintes fins:

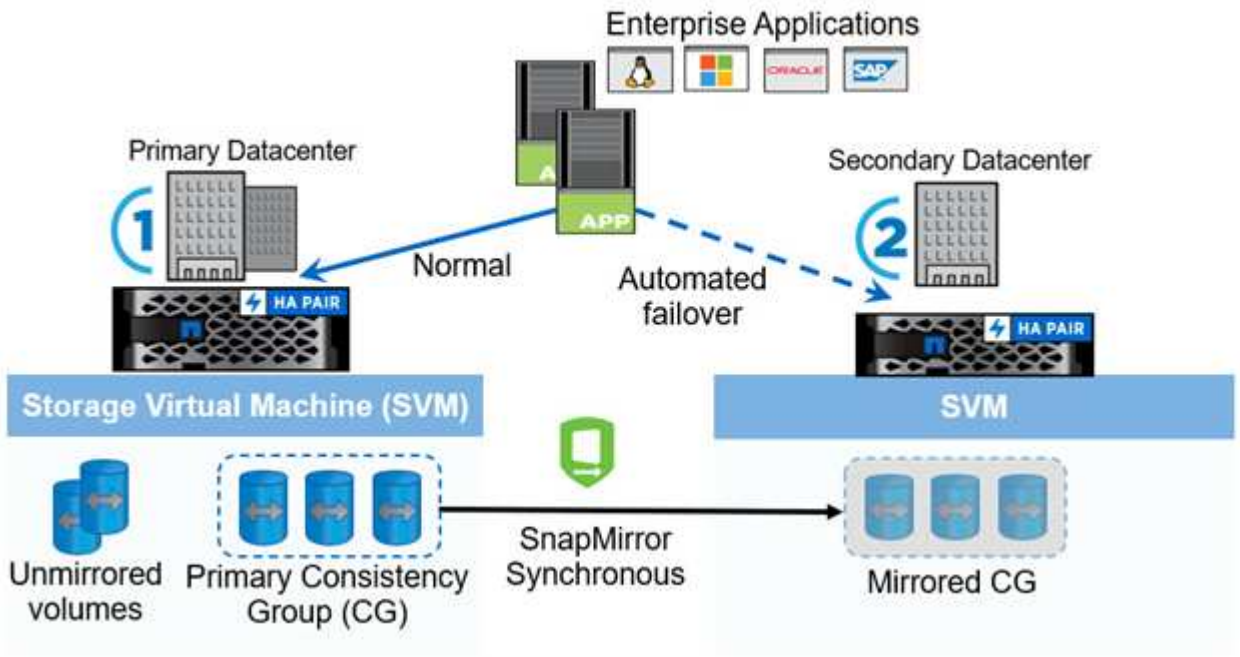
- Estabeleça um quórum
- Disponibilidade contínua por failover automático (AUFO)
- Failovers planejados (PFO)

> O ONTAP Mediator 1,7 pode gerenciar dez pares de cluster com o objetivo de continuidade dos negócios.

Quando o Mediador ONTAP não está disponível, não é possível executar failovers planejados ou automatizados. Os dados da aplicação continuam a replicar de forma síncrona, sem interrupções, para zero perda de dados.

Operações

A figura a seguir ilustra o design da sincronização ativa do SnapMirror em alto nível.



O diagrama mostra uma aplicação empresarial hospedada em uma VM de storage (SVM) no data center primário. O SVM contém cinco volumes, três dos quais fazem parte de um grupo de consistência. Os três volumes no grupo de consistência são espelhados para um data center secundário. Em circunstâncias normais, todas as operações de gravação são executadas no data center principal; na verdade, esse data center serve como fonte para operações de e/S, enquanto o data center secundário serve como destino.

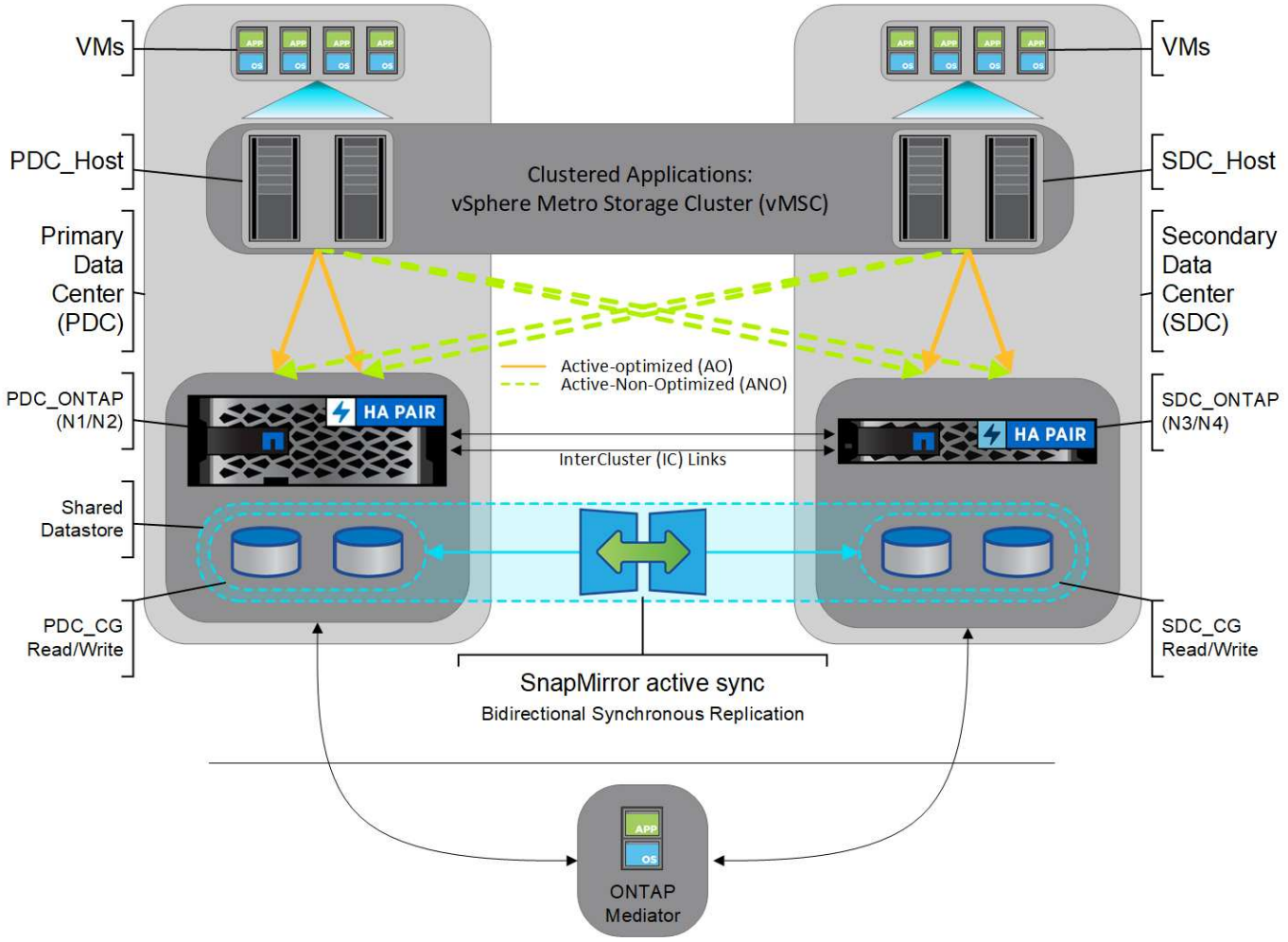
No caso de um cenário de desastre no data center principal, o ONTAP direciona o data center secundário para atuar como o principal, atendendo a todas as operações de e/S. Apenas os volumes que são espelhados no grupo consistência são servidos. Qualquer operação pertencente aos outros dois volumes na SVM será afetada pelo evento de desastre.

Ativo-ativo simétrico

O SnapMirror active Sync oferece soluções assimétricas e simétricas.

Em *configurações assimétricas*, a cópia de armazenamento primário expõe um caminho otimizado para ativos e serve ativamente e/S do cliente O local secundário usa um caminho remoto para e/S Os caminhos de storage do local secundário são considerados ativos-não-otimizados. O acesso ao LUN de gravação é maximizado a partir do site secundário.

Em *configurações ativas/ativas simétricas*, os caminhos otimizados para ativos são expostos em ambos os locais, são específicos do host e são configuráveis, o que significa que os hosts de ambos os lados podem acessar o storage local para e/S ativa



Ativo-ativo simétrico é destinado a aplicativos em cluster, incluindo VMware Metro Storage Cluster, Oracle RAC e Cluster de failover do Windows com SQL.

Casos de uso para sincronização ativa do SnapMirror

As demandas de um ambiente de negócios globalmente conectado exigem recuperação rápida de dados de aplicações essenciais aos negócios, sem perda de dados no caso de uma interrupção, como um ataque cibernético, uma interrupção de energia ou um desastre natural. Essas demandas são intensificadas em áreas como finanças e aquelas que aderiram a mandatos regulatórios, como o Regulamento Geral de proteção de dados (GDPR).

A sincronização ativa do SnapMirror fornece os seguintes casos de uso:

Implantação de aplicativos para objetivo de tempo de recuperação zero (rto)

Em uma implantação de sincronização ativa do SnapMirror, você tem um cluster primário e secundário. Um LUN no cluster primário `1LP`) tem um espelho (`L1s`) no secundário; ambos os LUNs compartilham o mesmo ID de série e são relatados como LUNs de leitura e gravação no host. No entanto, as operações de leitura e gravação só são atendidas no LUN primário `1LP`, . Todas as gravações no espelho `L1S` são servidas por proxy.

Implantação de aplicações para rto zero ou failover transparente de aplicações (TAF)

O TAF é baseado no failover de caminho baseado em software MPIO de host para obter acesso sem

interrupções ao storage. Ambas as cópias LUN - por exemplo, cópia primária (L1P) e cópia espelhada (L1S) - têm a mesma identidade (número de série) e são reportadas como graváveis para leitura para o host. No entanto, as leituras e gravações são atendidas apenas pelo volume primário. I/os emitidos para a cópia espelhada são proxied para a cópia primária. O caminho preferido do host para L1 é VS1:N1 com base no estado de acesso otimizado ativo (A/o) de acesso por unidade lógica assimétrica (ALUA). O Mediador ONTAP é necessário como parte da implantação, principalmente para executar failover (planejado ou não planejado) em caso de uma interrupção de storage no primário.

O SnapMirror ative Sync usa o ALUA, um mecanismo que permite que um software de multipathing host de aplicativos com caminhos anunciados com prioridades e disponibilidade de acesso para a comunicação do host de aplicativos com o storage array. O ALUA marca caminhos otimizados ativos para os controladores que possuem o LUN e outros como caminhos não otimizados ativos, usados somente se o caminho primário falhar.

Aplicações em cluster

Os aplicativos em cluster, incluindo VMware Metro Storage Cluster, Oracle RAC e Windows failover Clustering com SQL, exigem acesso simultâneo para que as VMs possam ser reexecutadas em outro local sem qualquer sobrecarga de desempenho. O SnapMirror ativo-ativo simétrico do SYNC ativo serve a e/S localmente com replicação bidirecional para atender aos requisitos de aplicações em cluster.

Cenário de desastre

Replique sincronamente vários volumes para uma aplicação entre locais em locais geograficamente dispersos. Você pode fazer o failover automaticamente para a cópia secundária em caso de interrupção do primário, permitindo a continuidade dos negócios das aplicações de camada um. Quando o site que hospeda o cluster primário sofre um desastre, o software de multipathing do host marca todos os caminhos pelo cluster como inativos e usa caminhos do cluster secundário. O resultado é um failover sem interrupções habilitado pelo ONTAP Mediator para a cópia espelhada.

Failover do Windows

O SnapMirror active Sync oferece flexibilidade com granularidade fácil de usar no nível da aplicação e failover automático. O SnapMirror active Sync usa replicação síncrona comprovada da SnapMirror em rede IP para replicar dados em alta velocidade via LAN ou WAN, para obter alta disponibilidade de dados e rápida replicação de dados para seus aplicativos essenciais aos negócios, como Oracle, Microsoft SQL Server e assim por diante, em ambientes virtuais e físicos.

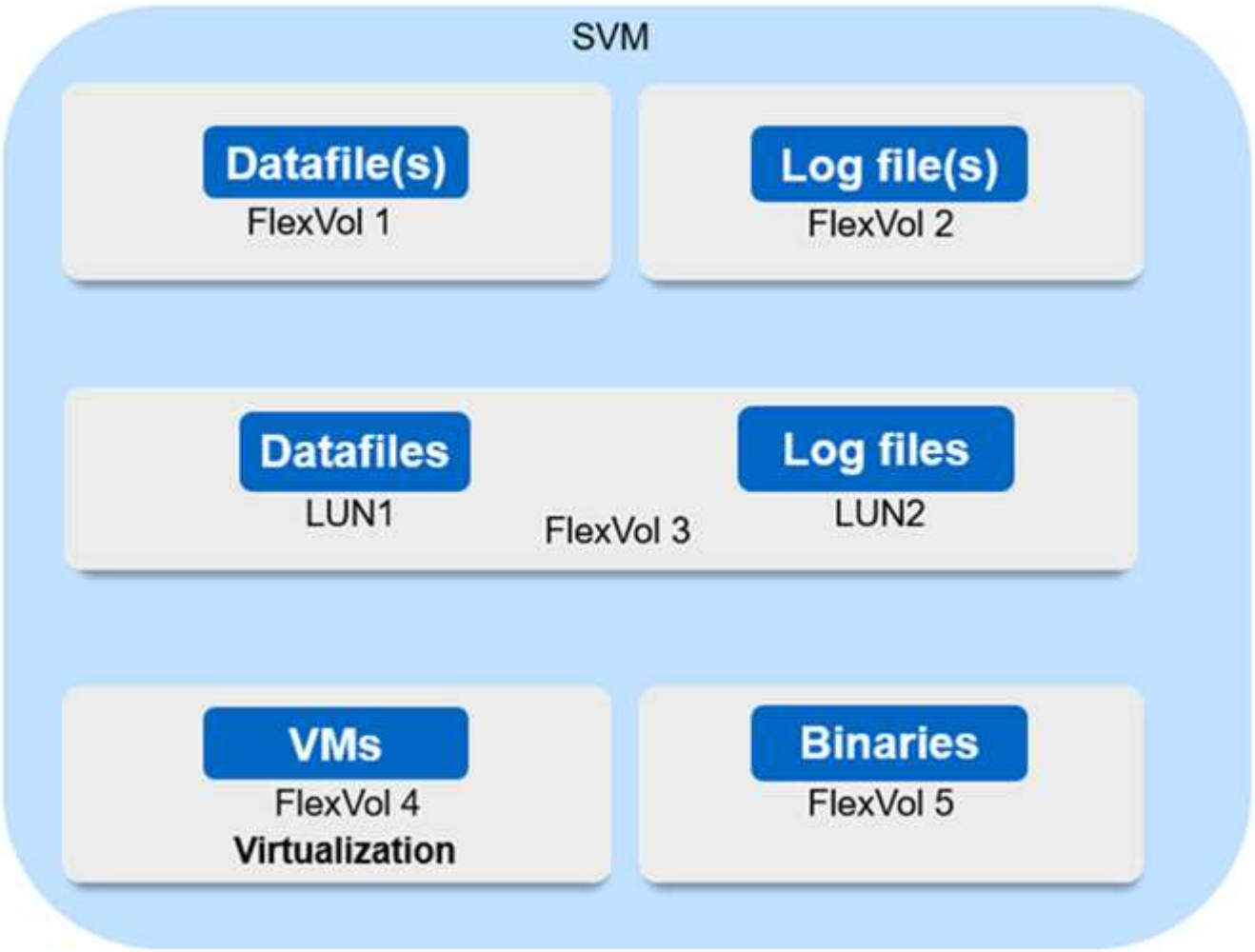
O SnapMirror ative Sync permite que os serviços de negócios essenciais continuem operando mesmo com uma falha completa do local, com o TAF para a cópia secundária. Nenhuma intervenção manual ou nenhum script adicional é necessário para acionar esse failover.

Estratégia de implantação e práticas recomendadas para a sincronização ativa do SnapMirror

É importante que sua estratégia de proteção de dados identifique claramente as ameaças aos workloads que precisam ser protegidas para manter a continuidade dos negócios. A etapa mais importante na estratégia de proteção de dados é ter clareza no layout de dados de aplicações empresariais para que você possa decidir como distribuir os volumes e proteger a continuidade dos negócios. Como o failover ocorre no nível do grupo de consistência por aplicação, adicione os volumes de dados necessários ao grupo de consistência.

Configuração SVM

O diagrama captura uma configuração recomendada de VM de storage (SVM) para sincronização ativa do SnapMirror.



- Para volumes de dados:
  - Cargas de trabalho de leitura aleatória são isoladas de gravações sequenciais; portanto, dependendo do tamanho do banco de dados, os dados e arquivos de log são normalmente colocados em volumes separados.
    - Para grandes bancos de dados críticos, o único arquivo de dados está no FlexVol 1 e seu arquivo de log correspondente está no FlexVol 2.
    - Para uma melhor consolidação, bancos de dados não críticos de tamanho pequeno a médio são agrupados de modo que todos os arquivos de dados estejam no FlexVol 1 e seus arquivos de log correspondentes estejam no FlexVol 2. No entanto, você perderá a granularidade no nível do aplicativo por meio desse agrupamento.
  - Outra variante é ter todos os arquivos dentro do mesmo FlexVol 3, com arquivos de dados em LUN1 e seus arquivos de log em LUN 2.
- Se o seu ambiente for virtualizado, você terá todas as VMs para vários aplicativos empresariais compartilhados em um datastore. Normalmente, as VMs e os binários da aplicação são replicados assincronamente usando o SnapMirror.

Plano

Pré-requisitos

Ao Planejar sua implantação de sincronização ativa do SnapMirror, verifique se você atendeu aos vários requisitos de hardware, software e configuração do sistema.

Hardware

- Somente clusters de HA de dois nós são compatíveis.
- Ambos os clusters precisam ser AFF (A-Series e C-Series) ou ASA (A-Series e C-Series). A mistura entre AFF e ASA não é suportada. A replicação é suportada entre o AFF A-Series e o C-Series.

Software

- ONTAP 9.9,1 ou posterior
- ONTAP Mediador 1,2 ou posterior
- Um servidor Linux ou máquina virtual para o Mediador ONTAP executando um dos seguintes:

ONTAP versão mediadora	Versões Linux suportadas
1,9	• Red Hat Enterprise Linux ◦ Compatível: 8,4, 8,5, 8,6, 8,7, 8,9, 9,1 e 9,3 1 ◦ Recomendado: 8,8, 8,10, 9,0, 9,2, 9,4 e 9,5 • Rocky Linux 8 e 9
1,8	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4 • Rocky Linux 8 e 9
1,7	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Rocky Linux 8 e 9
1,6	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2 • Rocky Linux 8 e 9
1,5	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,4	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,3	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3 • CentOS: 7,6, 7,7, 7,8, 7,9
1,2	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1 • CentOS: 7,6, 7,7, 7,8, 7,9

1. Compatível significa que o RHEL não suporta mais esta versão, mas o ONTAP Mediator ainda pode ser instalado.

Licenciamento

- A licença síncrona do SnapMirror deve ser aplicada em ambos os clusters.
- A licença do SnapMirror deve ser aplicada em ambos os clusters.

> Se os sistemas de storage da ONTAP tiverem sido adquiridos antes de junho de 2019, consulte "Chaves de licença principal do NetApp ONTAP" para obter a licença síncrona SnapMirror necessária.

Ambiente de rede

- O tempo de ida e volta (RTT) de latência entre clusters deve ser inferior a 10 milissegundos.
- A partir do ONTAP 9.14,1, "Reservas persistentes SCSI-3" são suportados com a sincronização ativa do SnapMirror.

Protocolos compatíveis

- Somente protocolos SAN são compatíveis (não NFS/SMB).
- Apenas são suportados protocolos Fibre Channel e iSCSI.
- O espaço IPspace padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos de pares de cluster. IPspace personalizado não é suportado.

Estilo de segurança NTFS

O estilo de segurança NTFS é **não** suportado em volumes de sincronização ativos do SnapMirror.

ONTAP Mediador

- O Mediador ONTAP deve ser provisionado externamente e anexado ao ONTAP para failover transparente de aplicativos.
- Para estar totalmente funcional e habilitar o failover automático não planejado, o mediador externo do ONTAP deve ser provisionado e configurado com clusters do ONTAP.
- O Mediador ONTAP deve ser instalado em um terceiro domínio de falha, separado dos dois clusters ONTAP.
- Ao instalar o Mediador ONTAP, você deve substituir o certificado autoassinado por um certificado válido assinado por uma CA confiável convencional.
- Para obter mais informações sobre o Mediador ONTAP, "Prepare-se para instalar o serviço Mediador ONTAP"consulte .

Volumes de destino de leitura-gravação

- As relações de sincronização ativa do SnapMirror não são compatíveis com volumes de destino de leitura e gravação. Antes de usar um volume de leitura e gravação, você deve convertê-lo em um volume DP criando uma relação de SnapMirror em nível de volume e excluindo a relação. Para obter detalhes, "Converta relações SnapMirror existentes para a sincronização ativa do SnapMirror"consulte .

Mais informações

- "Hardware Universe"
- "Visão geral do Mediador ONTAP"

Interoperabilidade de sincronização ativa do SnapMirror

O SnapMirror ative Sync é compatível com vários sistemas operacionais, hosts de aplicativos e outros recursos do ONTAP.

Para obter detalhes específicos de capacidade de suporte e interoperabilidade não abordados aqui, consulte a ferramenta de Matriz de interoperabilidade ("IMT").

Hosts de aplicativos

Os hosts de aplicativos de suporte a sincronização ativa do SnapMirror incluem Hyper-V, Red Hat Enterprise Linux (RHEL), VMware, VMware vSphere Metro Storage Cluster (vMSC), Windows Server e, a partir do ONTAP 9.14,1, cluster de failover de servidor do Windows.

Sistemas operacionais

O SnapMirror ative Sync é compatível com vários sistemas operacionais, incluindo:

- AIX via PVR (Início ONTAP 9.11,1)
- HP-UX (Início do ONTAP 9.10,1)
- Solaris 11,4 (Início do ONTAP 9.10,1)

AIX

A partir do ONTAP 9.11,1, o AIX é suportado com a sincronização ativa do SnapMirror via PVR.

O SnapMirror active Sync pode fornecer proteção de dados RPO zero, mas o processo de failover com AIX requer etapas adicionais para reconhecer a alteração de caminho. Os LUNs que não fazem parte de um grupo de volume raiz terão uma pausa de e/S até que um `cfgmgr` comando seja executado. Isso pode ser automatizado, e a maioria dos aplicativos retomará as operações sem interrupções adicionais.

Os LUNs que fazem parte de um grupo de volumes raiz geralmente não devem ser protegidos com a sincronização ativa do SnapMirror. Não é possível executar o `cfgmgr` comando após um failover, o que significa que uma reinicialização é necessária para reconhecer as alterações nos caminhos SAN. Você ainda pode alcançar a proteção de dados RPO zero do grupo de volume raiz, mas o failover causará interrupções.

Consulte sua equipe de conta do NetApp para obter mais informações sobre a sincronização ativa do SnapMirror com o AIX.

HP-UX

A partir do ONTAP 9.10,1, é suportada a sincronização ativa do SnapMirror para HP-UX.

Failover automático não planejado com HP-UX

Um evento de failover não planejado automático (AUFO) no cluster mestre isolado pode ser causado por falha de evento duplo quando a conexão entre o cluster primário e o cluster secundário é perdida e a conexão entre o cluster primário e o mediador também é perdida. Este é considerado um evento raro, ao contrário de outros eventos AUFO.

- Nesse cenário, pode levar mais de 120 segundos para que a I/o seja retomada no host HP-UX. Dependendo dos aplicativos que estão sendo executados, isso pode não levar a interrupções de e/S ou mensagens de erro.
- Para remediar, é necessário reiniciar os aplicativos no host HP-UX que tenham uma tolerância de interrupção inferior a 120 segundos.

Solaris

A partir do ONTAP 9.10,1, o SnapMirror ative Sync suporta o Solaris 11,4.

Para garantir que os aplicativos clientes Solaris não sejam disruptivos quando ocorrer um switchover não planejado de failover de local em um ambiente de sincronização ativa do SnapMirror, modifique as configurações padrão do Solaris os. Para configurar o Solaris com as configurações recomendadas, consulte o artigo da base de dados de Conhecimento "Configurações recomendadas no SnapMirror ative Sync".

Interoperabilidade do ONTAP

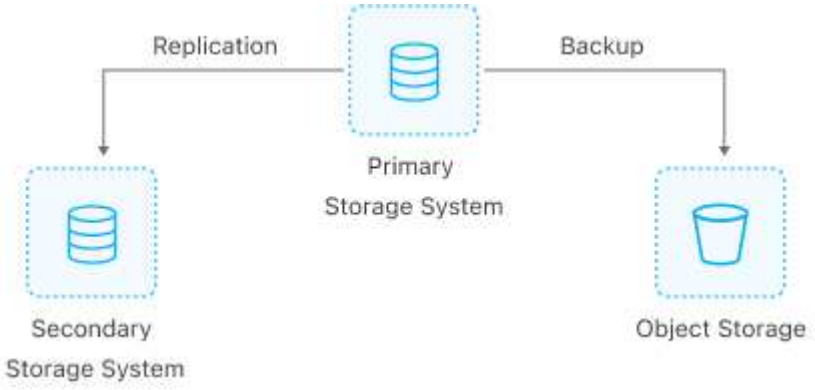
O SnapMirror active Sync integra-se a componentes do ONTAP para estender seus recursos de proteção de dados.

FabricPool

O SnapMirror active Sync é compatível com volumes de origem e destino em agregados FabricPool com políticas de disposição em camadas Nenhuma, Snapshot ou automática. O SnapMirror active Sync não é compatível com agregados FabricPool usando uma política de disposição em camadas.

Configurações de fan-out

No configurações de fan-out, o volume de origem pode ser espelhado em um ponto de extremidade de destino de sincronização ativa do SnapMirror e em um ou mais relacionamentos assíncronos do SnapMirror.



A sincronização ativa do SnapMirror é compatível configurações de fan-out com a `MirrorAllSnapshots` política e, a partir do ONTAP 9.11,1, a `MirrorAndVault` política. As configurações de fan-out não são suportadas na sincronização ativa do SnapMirror com a `XDPDefault` política.

A partir do ONTAP 9.15,1, o SnapMirror ative Sync suporta reconfiguração automática na etapa fan-out após um evento de failover. Se o failover do local primário para o local secundário tiver sido bem-sucedido, o local terciário será reconfigurado automaticamente para tratar o local secundário como a origem. A reconfiguração é acionada por um failover planejado ou não planejado. A reconfiguração também ocorre após o failback para o site primário.

Para obter informações sobre como gerenciar sua configuração de fan-out em versões anteriores do ONTAP,

retomar a proteção na configuração de fan-outconsulte .

Restauração NDMP

A partir do ONTAP 9.13,1, você pode usar NDMP para copiar e restaurar dados com a sincronização ativa do SnapMirror. O uso do NDMP permite que você mova dados para a fonte de sincronização ativa do SnapMirror para concluir uma restauração sem pausar a proteção. Isso é particularmente útil em configurações de fan-out.

SnapCenter

A sincronização ativa do SnapMirror é suportada com o SnapCenter a partir "SnapCenter 5,0"do . O SnapCenter permite a criação de snapshots que podem ser usados para proteger e recuperar aplicativos e máquinas virtuais, permitindo soluções de armazenamento sempre disponíveis com granularidade no nível do aplicativo.

SnapRestore

O SnapMirror ative Sync é compatível com SnapRestore de arquivo único e parcial.

SnapRestore de um único arquivo

A partir do ONTAP 9.11,1, Single-file SnapRestore é compatível com volumes de sincronização ativos do SnapMirror. É possível restaurar um único arquivo de uma cópia Snapshot replicada da fonte de sincronização ativa do SnapMirror para o destino. Como os volumes podem conter um ou mais LUNs, esse recurso ajuda a implementar uma operação de restauração menos disruptiva, restaurando de maneira granular um único LUN sem interromper os outros LUNs. O Single File SnapRestore tem duas opções: In-place e out-of-place.

SnapRestore de arquivo parcial

A partir do ONTAP 9.12,1, "Restauração parcial de LUN" é compatível com volumes de sincronização ativos do SnapMirror. É possível restaurar os dados de cópias Snapshot criadas por aplicações que foram replicadas entre a fonte (volume) de sincronização ativa do SnapMirror e os volumes de destino (cópia Snapshot). LUN parcial ou restauração de arquivos pode ser necessária se você precisar restaurar um banco de dados em um host que armazena vários bancos de dados no mesmo LUN. O uso desta funcionalidade requer que você saiba o deslocamento de byte inicial da contagem de dados e bytes.

LUNs grandes e grandes volumes

O suporte para LUNs grandes e volumes grandes (maiores de 100 TB) depende da versão do ONTAP que você está usando e da sua plataforma.

ONTAP 9.12.1P2 e posterior

- Para o ONTAP 9.12,1 P2 e posterior, o SnapMirror ative Sync suporta LUNs grandes e volumes grandes superiores a 100 TB no ASA e no AFF (Série A e Série C). Os clusters primário e secundário devem ser do mesmo tipo: ASA ou AFF. É suportada a replicação do AFF A-Series para o AFF C-Series e vice-versa.

> Nas versões 9.12.1P2 e posteriores do ONTAP, você precisa garantir que os clusters primário e secundário sejam all-flash SAN Arrays (ASA) ou all-flash array (AFF) e que ambos tenham ONTAP 9.12,1 P2 ou posterior instalado. Se o cluster secundário estiver executando uma versão anterior ao ONTAP 9.12.1P2 ou se o tipo de array não for o mesmo que o cluster primário, a relação síncrona poderá ficar fora de sincronia se o volume primário aumentar acima de 100 TB.

ONTAP 9.9,1 - 9.12.1P1

- Para versões do ONTAP entre o ONTAP 9.9,1 e o 9.12.1 P1 (inclusive), LUNs grandes e volumes maiores que 100TB TB são compatíveis apenas com arrays all-flash SAN. É suportada a replicação do AFF A-Series para o AFF C-Series e vice-versa.

> Para versões do ONTAP entre o ONTAP 9.9,1 e o 9.12.1 P2, você deve garantir que os clusters primário e secundário sejam all-flash SAN arrays e que ambos tenham o ONTAP 9.9,1 ou posterior instalado. Se o cluster secundário estiver executando uma versão anterior ao ONTAP 9.9,1 ou se não for um array SAN all-flash, a relação síncrona poderá ficar fora de sincronia se o volume primário aumentar acima de 100 TB.

Mais informações

- "Como configurar um host AIX para sincronização ativa do SnapMirror"

Limites de objetos para sincronização ativa do SnapMirror

Ao se preparar para usar a sincronização ativa do SnapMirror, esteja ciente dos seguintes limites de objeto.

Grupos de consistência em um cluster

Os limites de grupo de consistência para um cluster com sincronização ativa do SnapMirror são calculados com base nas relações e dependem da versão do ONTAP usada. Os limites são independentes da plataforma.

Versão de ONTAP	Número máximo de relacionamentos
ONTAP 9.11,1 e posterior	50
ONTAP 9.10,1	20
ONTAP 9.9,1	5

Volumes por grupo de consistência

O número máximo de volumes por grupo de consistência com a sincronização ativa do SnapMirror é independente da plataforma.

Versão de ONTAP	Número máximo de volumes suportados em uma relação de grupo de consistência
ONTAP 9.15,1 e posterior	80
ONTAP 9.10,1-9.14.1	16
ONTAP 9.9,1	12

Volumes

Os limites de volume na sincronização ativa do SnapMirror são calculados com base no número de endpoints, e não no número de relacionamentos. Um grupo de consistência com 12 volumes contribui com 12 pontos de extremidade no cluster primário e secundário. As relações de sincronização ativa do SnapMirror e sincronização SnapMirror contribuem para o número total de endpoints.

Os pontos finais máximos por plataforma estão incluídos na tabela a seguir.

S. não	Plataforma	Pontos de extremidade por HA para sincronização ativa do SnapMirror			Pontos de extremidade de sincronização total e de sincronização ativa do SnapMirror por HA		
		ONTAP 9.11,1 e posterior	ONTAP 9.10,1	ONTAP 9.9,1	ONTAP 9.11,1 e posterior	ONTAP 9.10,1	ONTAP 9.9,1
1	AFF	400	200	60	400	200	80
2	ASA	400	200	60	400	200	80

Limites de objetos SAN

Os limites de objetos SAN estão incluídos na tabela a seguir. Os limites se aplicam independentemente da plataforma.

Objeto em uma relação de sincronização ativa do SnapMirror	Contar
LUNs por volume	256
Mapas LUN por nó	• 4096 (ONTAP 9.10 e posterior) • 2048 (ONTAP 9.9,1 e anteriores)
Mapas LUN por cluster	• 8192 (ONTAP 9.10 e posterior) • 4096 (ONTAP 9.9,1 e anteriores)
LIFs por SVM (com pelo menos um volume em uma relação de sincronização ativa do SnapMirror)	256
LIFs entre clusters por nó	4
LIFs inter-cluster por cluster	8

Informações relacionadas

- "Hardware Universe"
- "Limites do grupo de consistência"

Configurar

Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror utiliza clusters com permissões para garantir que seus dados estejam disponíveis no caso de um cenário de failover. O Mediador ONTAP é um recurso chave que garante a continuidade dos negócios, monitorando a integridade de cada cluster. Para configurar a sincronização ativa do SnapMirror, primeiro instale o Mediador do ONTAP e verifique se os clusters primário e secundário estão configurados corretamente.

Depois de instalar o Mediador do ONTAP e configurar os clusters, você deve [initialize-the-ontap-mediator]usar o Mediador do ONTAP para usar com a sincronização ativa do SnapMirror. Você deve então Crie, inicialize e mapeie o grupo de consistência para a sincronização ativa do SnapMirror.

ONTAP Mediador

O Mediador do ONTAP fornece um armazenamento persistente e vedado para metadados de alta disponibilidade (HA) usados pelos clusters do ONTAP em uma relação de sincronização ativa do SnapMirror. Além disso, o ONTAP Mediator fornece uma funcionalidade de consulta de integridade de nó síncrono para auxiliar na determinação de quórum e serve como proxy de ping para deteção de vivacidade do controlador.

Pré-requisitos para o Mediador ONTAP

- O Mediador ONTAP inclui seu próprio conjunto de pré-requisitos. Você deve atender a esses pré-requisitos antes de instalar o mediador.

  Para obter mais informações, "Prepare-se para instalar o serviço Mediador ONTAP"consulte .

- Por padrão, o Mediador ONTAP fornece serviço através da porta TCP 31784. Você deve garantir que a porta 31784 esteja aberta e disponível entre os clusters do ONTAP e o mediador.

Instale o Mediador ONTAP e confirme a configuração do cluster

Prossiga por cada uma das etapas a seguir. Para cada etapa, você deve confirmar se a configuração específica foi executada. Use o link incluído após cada etapa para obter mais informações, conforme necessário.

Passos

1. Instale o serviço do Mediador ONTAP antes de garantir que os clusters de origem e destino estejam configurados corretamente.

   Prepare-se para instalar ou atualizar o serviço do Mediador ONTAP

2. Confirme se existe uma relação de peering de cluster entre os clusters.

   > O espaço IPspace padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos de pares de cluster. Um espaço IPspace personalizado não é suportado.

   Configurar relações entre pares

3. Confirme se as VMs de armazenamento são criadas em cada cluster.

   Criação de um SVM

4. Confirme se existe uma relação de pares entre as VMs de armazenamento em cada cluster.

   Criando uma relação de peering SVM

5. Confirme se os volumes existem para os LUNs.

   Criando um volume

6. Confirme se pelo menos um SAN LIF é criado em cada nó no cluster.

   "Considerações para LIFs em um ambiente de SAN de cluster"

   "Criando um LIF"

7. Confirme se os LUNs necessários são criados e mapeados para um grupo, que é usado para mapear LUNs para o iniciador no host do aplicativo.

   Crie LUNs e mapeie grupos

8. Pode novamente o anfitrião de aplicações para descobrir quaisquer novos LUNs.

Inicialize o Mediador ONTAP para sincronização ativa do SnapMirror usando certificados autoassinados

Depois de instalar o Mediador ONTAP e confirmar a configuração do cluster, você deve inicializar o Mediador ONTAP para monitoramento de cluster. Você pode inicializar o Mediador ONTAP usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

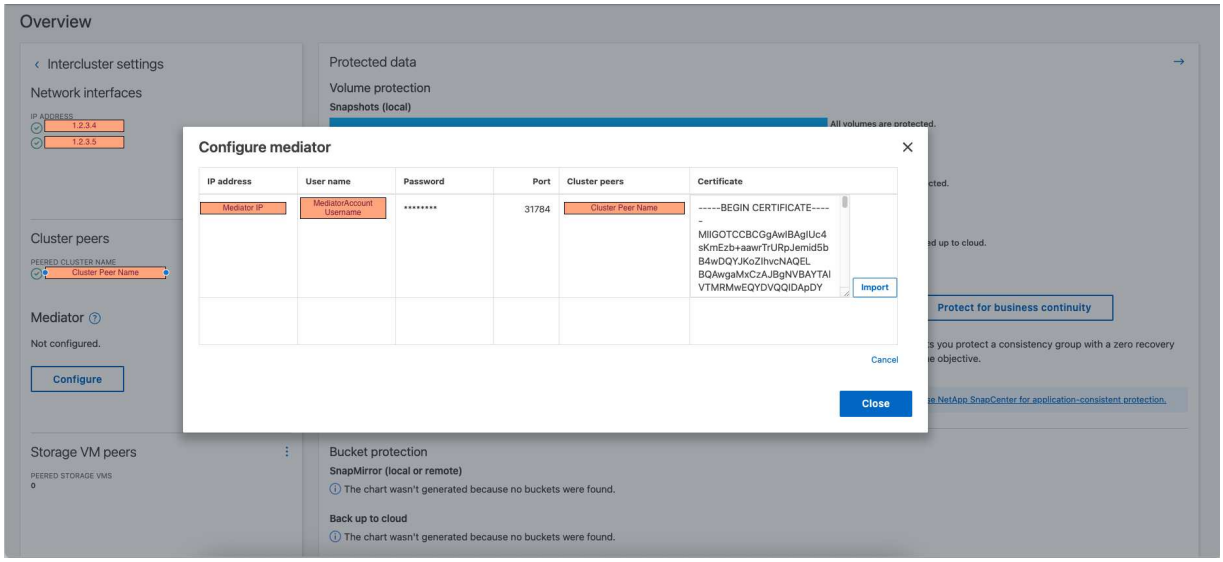
Com o Gerenciador de sistema, você pode configurar o servidor do ONTAP Mediator para failover automatizado. Você também pode substituir o SSL e a CA autoassinados pelo certificado SSL validado de terceiros e pela CA se ainda não o tiver feito.

> Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

Passos

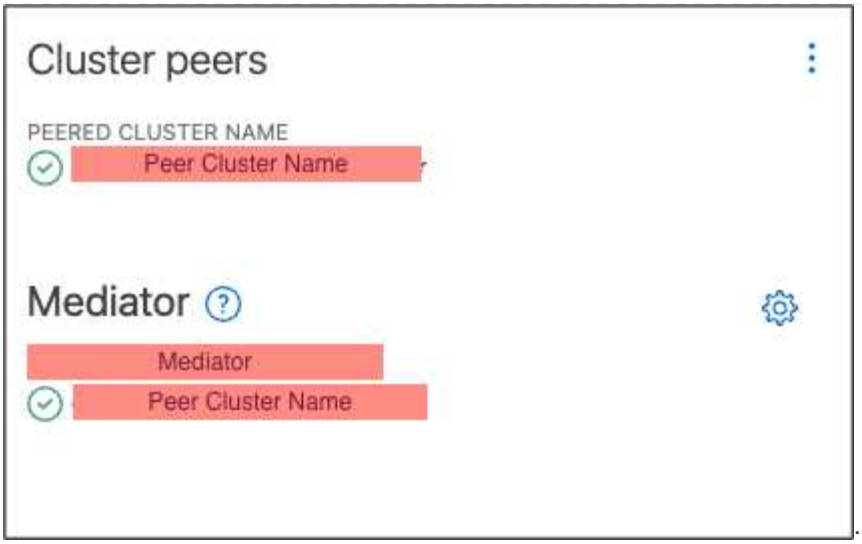
1. Navegue até **proteção > Visão geral > Mediador > Configurar**.
2. Selecione **Adicionar** e insira as seguintes informações do servidor do ONTAP Mediator:
   - Endereço IPv4
   - Nome de utilizador
   - Palavra-passe
   - Certificado
3. Você pode fornecer a entrada do certificado de duas maneiras:
   - **Opção (a)**: Selecione **Importar** para navegar para o `.crt` arquivo e importá-lo.
   - **Opção (b)**: Copie o conteúdo do `.crt` arquivo e cole no campo **certificado**.

   Quando todos os detalhes são inseridos corretamente, o certificado fornecido é instalado em todos os clusters de pares.



Quando a adição de certificado estiver concluída, o Mediador ONTAP é adicionado ao cluster ONTAP.

A imagem a seguir demonstra uma configuração bem-sucedida do ONTAP Mediator:



CLI

Você pode inicializar o Mediador ONTAP a partir do cluster primário ou secundário usando a CLI do ONTAP. Quando você emite o `mediator add` comando em um cluster, o Mediador ONTAP é adicionado automaticamente ao outro cluster.

Ao usar o Mediador para monitorar um relacionamento de sincronização ativa do SnapMirror, o Mediador não pode ser inicializado no ONTAP sem um certificado de autoridade de certificação (CA) ou autoassinado válido. Você adiciona um certificado válido ao armazenamento de certificados para clusters com permissões. Ao usar o Mediator para monitorar sistemas IP MetroCluster, o HTTPS não é usado após a configuração inicial; portanto, os certificados não são necessários.

Passos

1. Localize o certificado da CA do Mediador ONTAP no local de instalação do software de host/VM do ONTAP Mediator Linux `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Adicione uma autoridade de certificação válida ao armazenamento de certificados no cluster de permissões.

   Exemplo

   ```
   [root@ontap-mediator server_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
   BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
   …
   p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
   -----END CERTIFICATE-----
   ```

3. Adicione o certificado da CA do Mediador do ONTAP a um cluster do ONTAP. Quando solicitado, insira o certificado de CA obtido no Mediador ONTAP. Repita as etapas em todos os clusters de pares:

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

Exemplo

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator server_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. Exiba o certificado de CA autoassinado instalado usando o nome gerado do certificado:

   `security certificate show -common-name <common_name>`

   Exemplo

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- -------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                          ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. Inicialize o Mediador ONTAP em um dos clusters. O Mediador ONTAP é adicionado automaticamente para o outro cluster:

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Exemplo

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Verifique o status da configuração do Mediador ONTAP:

   `snapmirror mediator show`

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

   `Quorum Status` Indica se as relações de grupo de consistência do SnapMirror estão sincronizadas com o Mediador ONTAP; um status de `true` indica sincronização bem-sucedida.

Reinicie o ONTAP Mediator com certificados de terceiros

Talvez seja necessário reinicializar o serviço ONTAP Mediator. Pode haver situações que exigem a reinicialização do serviço do Mediador ONTAP, como uma alteração no endereço IP do Mediador ONTAP, expiração do certificado e muito mais.

O procedimento a seguir ilustra a reinicialização do Mediador ONTAP para um caso específico quando um certificado autoassinado precisa ser substituído por um certificado de terceiros.

Sobre esta tarefa

Você precisa substituir os certificados autoassinados do cluster SM-BC por certificados de terceiros, remover a configuração do Mediador ONTAP do ONTAP e, em seguida, adicionar o Mediador ONTAP.

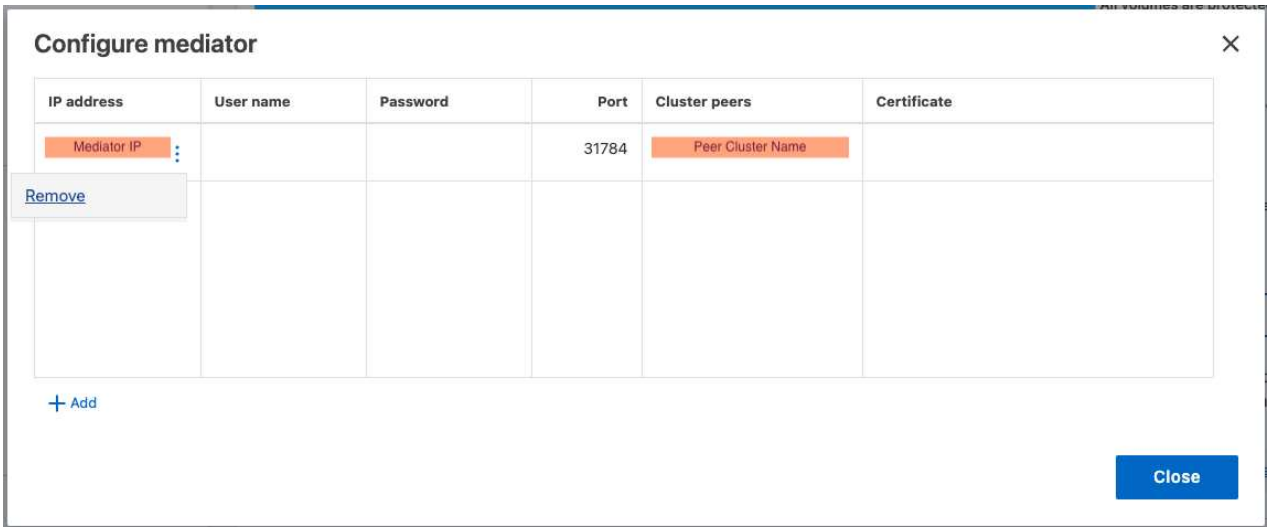
System Manager

Com o Gerenciador de sistema, você precisa remover o Mediador ONTAP configurado com o certificado autoassinado antigo do cluster ONTAP e reconfigurar o cluster ONTAP com o novo certificado de terceiros.

Passos

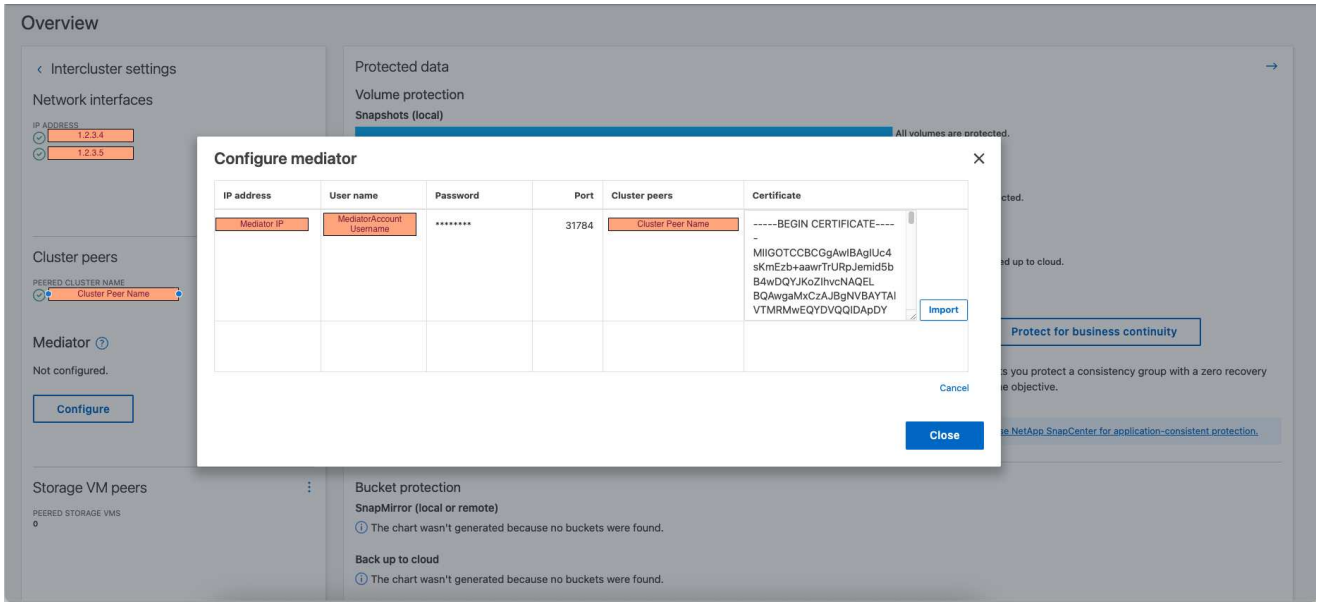
1. Selecione o ícone de opções de menu e selecione **Remover** para remover o Mediador ONTAP.

> Esta etapa não remove o servidor-CA autoassinado do cluster ONTAP. A NetApp recomenda navegar até a guia **certificado** e removê-lo manualmente antes de executar a próxima etapa abaixo para adicionar um certificado de terceiros:



2. Adicione o Mediador ONTAP novamente com o certificado correto.

O Mediador ONTAP está agora configurado com o novo certificado auto-assinado de terceiros.



CLI

Você pode reinicializar o Mediador do ONTAP a partir do cluster primário ou secundário usando a CLI do

ONTAP para substituir o certificado autoassinado pelo certificado de terceiros.

Passos

1. Remova o autoassinado instalado `ca.crt` anteriormente quando você usou certificados autoassinados para todos os clusters. No exemplo abaixo, há dois clusters:

   Exemplo

   ```
    C1_test_cluster::*> security certificate delete -vserver
   C1_test_cluster -common-name ONTAPMediatorCA
    2 entries were deleted.

    C2_test_cluster::*> security certificate delete -vserver
   C2_test_cluster -common-name ONTAPMediatorCA *
    2 entries were deleted.
   ```

2. Remova o Mediador ONTAP configurado anteriormente do cluster SM-BC usando `-force true`:

   Exemplo

   ```
   C1_test_cluster::*> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   1.2.3.4          C2_test_cluster   connected         true

   C1_test_cluster::*> snapmirror mediator remove -mediator-address
   1.2.3.4 -peer-cluster C2_test_cluster -force true

   Warning: You are trying to remove the ONTAP Mediator configuration
   with force. If this configuration exists on the peer cluster, it
   could lead to failure of a SnapMirror failover operation. Check if
   this configuration
            exists on the peer cluster C2_test_cluster and remove it as
   well.
   Do you want to continue? {y|n}: y

   Info: [Job 136] 'mediator remove' job queued

   C1_test_cluster::*> snapmirror mediator show
   This table is currently empty.
   ```

3. Consulte as etapas descritas em "Substitua certificados autoassinados por certificados de terceiros confiáveis" sobre como obter certificados da CA subordinada, referida como `ca.crt`. Substitua certificados autoassinados por certificados de terceiros confiáveis

O `ca.crt` tem certas propriedades derivadas da solicitação que precisam ser enviadas à autoridade PKI, definida no arquivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`.

4. Adicione o novo certificado de CA do Mediador ONTAP de terceiros `ca.crt` a partir do local de instalação do software de VM/host do ONTAP Mediator:

   Exemplo

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
   [root@ontap-mediator server_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
   BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
   …
   p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
   -----END CERTIFICATE-----
   ```

5. Adicione o `ca.crt` arquivo ao cluster de Contatos. Repita esta etapa para todos os clusters de pares:

   Exemplo

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
MIIFxTCCA62gAwIBAgIJANhtjk6HFCiOMA0GCSqGSIb3DQEBCwUAMHgxFTATBgNV
BAoMDE5ldEFwcCwgSW5jLjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3Ju
…
p+jdg5bG61cxkuvbRm7ykFbih1b88/Sgu5XJg2KRhjdISF98I81N+Fo=
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Remova o Mediador ONTAP configurado anteriormente do cluster de sincronização ativa do SnapMirror:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Adicione o Mediador ONTAP novamente:

   Exemplo

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

`Quorum Status` Indica se as relações do grupo de consistência do SnapMirror estão sincronizadas com o mediador; um status de `true` indica a sincronização bem-sucedida.

Proteja com a sincronização ativa do SnapMirror

O SnapMirror ative Sync oferece proteção assimétrica e, a partir do ONTAP 9.15,1, proteção ativa/ativa simétrica.

Configurar a proteção assimétrica

A configuração de proteção assimétrica usando a sincronização ativa do SnapMirror envolve a seleção de LUNs no cluster de origem do ONTAP e a adição a um grupo de consistência.

Antes de começar

- Você precisa ter uma licença síncrona do SnapMirror.
- Você deve ser um administrador de cluster ou VM de storage.
- Todos os volumes constituintes de um grupo de consistência precisam estar em uma única VM de storage (SVM).
  - Os LUNs podem residir em volumes diferentes.
- O cluster de origem e destino não pode ser o mesmo.
- Não é possível estabelecer relações de grupo de consistência de sincronização ativa do SnapMirror entre clusters do ASA e clusters que não sejam do ASA.
- O espaço IPspace padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos de pares de cluster. IPspace personalizado não é suportado.
- O nome do grupo de consistência deve ser único.
- Os volumes no cluster secundário (destino) devem ser do tipo DP.
- Os SVMs primário e secundário devem estar em uma relação de Contato.

Passos

Você pode configurar um grupo de consistência usando a CLI do ONTAP ou o Gerenciador do sistema.

A partir do ONTAP 9.10,1, o ONTAP oferece um endpoint de grupo de consistência e um menu no Gerenciador de sistemas, oferecendo utilitários de gerenciamento adicionais. Se estiver a utilizar o ONTAP 9.10,1 ou posterior, consulte "Configurar um grupo de consistência" "configurar a proteção"para criar uma relação de sincronização ativa do SnapMirror.

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

System Manager

1. No cluster principal, navegue até **proteção > Visão geral > proteger para continuidade de negócios > proteger LUNs**.
2. Selecione os LUNs que pretende proteger e adicione-os a um grupo de proteçãoão.
3. Selecione o cluster de destino e o SVM.
4. **Initialize Relationship** é selecionado por padrão. Clique em **Save** para iniciar a proteção.
5. Vá para **Dashboard > Performance** para verificar a atividade de IOPS dos LUNs.
6. No cluster de destino, use o System Manager para verificar se a proteção para o relacionamento de continuidade de negócios está em sincronia: **Proteção > relacionamentos**.

CLI

1. Crie uma relação de grupo de consistência a partir do cluster de destino.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   Você pode mapear até 12 volumes constituintes usando o `cg-item-mappings` parâmetro no `snapmirror create` comando.

   O exemplo a seguir cria dois grupos de consistência: `cg_src_ on the source with `vol1` E `vol2` um grupo de consistência de destino espelhado `cg_dst`, .

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. No cluster de destino, inicialize o grupo de consistência.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. Confirme se a operação de inicialização foi concluída com êxito. O estado deve ser `InSync`.

   ```
   snapmirror show
   ```

4. Em cada cluster, crie um grupo para que você possa mapear LUNs para o iniciador no host do aplicativo.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*
5. Em cada cluster, mapeie LUNs para o grupo:

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. Verifique se o mapeamento LUN foi concluído com êxito com o `lun map` comando. Depois, você pode descobrir os novos LUNs no host de aplicativos.

Configurar a proteção ativo-ativo simétrica

Você pode estabelecer proteção simétrica usando o Gerenciador do sistema ou a CLI do ONTAP. Em ambas

as interfaces, existem diferentes etapas para configurações uniformes e não uniformes.

Antes de começar

- Ambos os clusters devem estar executando o ONTAP 9.15,1 ou posterior.
- Configurações ativo-ativo simétricas exigem a `AutomatedFailoverDuplex` política de proteção. Como alternativa, você pode Crie uma política de SnapMirror personalizada fornecer o `-type` is `automated-failover-duplex`.

Exemplo 34. Passos

System Manager

Passos para uma configuração uniforme

1. No local principal, "Crie um grupo de consistência usando novos LUNs."
   a. Ao criar o grupo de consistência, especifique iniciadores de host para criar grupos.
   b. Marque a caixa de seleção para **Ativar SnapMirror** e escolha a `AutomatedFailoverDuplex` política.
   c. Na caixa de diálogo exibida, marque a caixa de seleção **Replique grupos de iniciadores** para replicar grupos de iniciadores. Em **Editar configurações proximais**, defina SVMs proximais para seus hosts.
   d. Selecione **Guardar**.

Passos para uma configuração não uniforme

1. No local principal, "Crie um grupo de consistência usando novos LUNs."
   a. Ao criar o grupo de consistência, especifique iniciadores de host para criar grupos.
   b. Marque a caixa de seleção para **Ativar SnapMirror** e escolha a `AutomatedFailoverDuplex` política.
   c. Selecione **Salvar** para criar os LUNs, o grupo de consistência, o grupo igrop, a relação SnapMirror e o mapeamento do grupo igrop.
2. No site secundário, crie um igrop e mapeie os LUNs.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione **Adicionar** para criar um novo grupo.
   c. Forneça um **Nome**, selecione **sistema operacional anfitrião** e, em seguida, escolha **Membros do Grupo Iniciador**.
   d. Selecione **Guardar**.
3. Mapeie o novo grupo para os LUNs de destino.
   a. Navegue até **armazenamento** > **LUNs**.
   b. Selecione todos os LUNs para mapear para o grupo.
   c. Selecione **More** (mais) e depois **Map to Initiator Groups (mapa para grupos de iniciadores)**.

CLI

Passos para uma configuração uniforme

1. Crie uma nova relação do SnapMirror agrupando todos os volumes na aplicação. Certifique-se de designar a `AutomatedFailOverDuplex` política para estabelecer replicação de sincronização bidirecional.

   ```
   snapmirror create -source-path source_path -destination-path
   destination_path -cg-item-mappings source_volume:@destination_volume
   -policy AutomatedFailOverDuplex
   ```

2. Confirme se a operação foi bem-sucedida, aguardando que o `Mirrored State` mostre como `SnapMirrored` e `Relationship Status` as `Insync`.

   ```
   snapmirror show -destination-path destination_path
   ```

3. No seu host, configure a conectividade de host com acesso a cada cluster de acordo com suas necessidades.
4. Estabeleça a configuração do grupo. Defina os caminhos preferidos para iniciadores no cluster local. Especifique a opção para replicar a configuração para a afinidade inversa do cluster de pares.

   ```
   SiteA::> igroup create -vserver svm_name -os-type os_type -igroup
   igroup_name -replication-peer peer_svm_name -initiator host

   SiteA::> igroup add -vserver svm_name -igroup igroup_name -os-type os_type
   -initiator host
   ```

5. A partir do host, descubra os caminhos e verifique se os hosts têm um caminho ativo/otimizado para o LUN de storage a partir do cluster preferido.
6. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters para alcançar o balanceamento de carga necessário.

Passos para uma configuração não uniforme

1. Crie uma nova relação do SnapMirror agrupando todos os volumes na aplicação. Certifique-se de designar a política "AutomatedFailOverDuplex" para estabelecer replicação de sincronização bidirecional.

   ```
   snapmirror create -source-path source_path -destination-path
   destination_path -cg-item-mappings source_volume:@destination_volume
   -policy AutomatedFailOverDuplex
   ```

2. Confirme se a operação foi bem-sucedida, aguardando que o `Mirrored State` mostre como `SnapMirrored` e `Relationship Status` as `Insync`.

   ```
   snapmirror show -destination-path destination_path
   ```

3. No seu host, configure a conectividade de host com acesso a cada cluster de acordo com suas necessidades.
4. Estabeleça as configurações do igrupo nos clusters de origem e destino.

   ```
   # primary site
   SiteA::> igroup create -vserver svm_name -igroup igroup_name -initiator
   host_1_name

   # secondary site
   SiteB::> igroup create -vserver svm_name -igroup igroup_name -initiator
   host_2_name
   ```

5. A partir do host, descubra os caminhos e verifique se os hosts têm um caminho ativo/otimizado para o LUN de storage a partir do cluster preferido.
6. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters para alcançar o balanceamento de carga necessário.

Converta uma relação existente do SnapMirror para uma relação de sincronização ativa do SnapMirror

Se tiver configurado a proteção SnapMirror, poderá converter a relação para a

sincronização ativa do SnapMirror. A partir do ONTAP 9.15,1, você pode converter a relação para usar proteção ativa/ativa simétrica.

Converta uma relação SnapMirror existente em uma relação de sincronização ativa assimétrica do SnapMirror

Se você tiver uma relação síncrona SnapMirror existente entre um cluster de origem e destino, poderá convertê-la em uma relação de sincronização ativa assimétrica do SnapMirror. Isso permite associar os volumes espelhados a um grupo de consistência, garantindo RPO zero em um workload de vários volumes. Além disso, você pode reter snapshots existentes do SnapMirror se precisar reverter para um ponto no tempo antes de estabelecer a relação de sincronização ativa do SnapMirror.

Sobre esta tarefa

- Você precisa ser um administrador de cluster e SVM nos clusters primário e secundário.
- Você não pode converter RPO zero para sincronização rto zero alterando a política de SnapMirror.
- Você deve garantir que os LUNs não estejam mapeados antes de emitir o `snapmirror create` comando.

  Se os LUNs existentes no volume secundário forem mapeados e a `AutomatedFailover` política estiver configurada, o `snapmirror create` comando acionará um erro.

Antes de começar

- Uma relação de sincronização com SnapMirror RPO zero deve existir entre o cluster primário e o secundário.
- Todos os LUNs no volume de destino devem ser não mapeados antes que a relação zero rto SnapMirror possa ser criada.
- O SnapMirror active Sync só é compatível com protocolos SAN (não NFS/CIFS). Certifique-se de que nenhum componente do grupo de consistência está montado para acesso nas.

Passos

1. A partir do cluster secundário, execute uma atualização do SnapMirror sobre a relação existente:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verifique se a atualização do SnapMirror foi concluída com êxito:

   ```
   SiteB::>snapmirror show
   ```

3. Pausar cada um dos relacionamentos síncronos com RPO zero:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Exclua cada uma das relações síncronas com RPO zero:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Libere a relação de origem do SnapMirror, mas mantenha as cópias Snapshot comuns:

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Crie uma relação síncrona de rto SnapMirror zero:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. Ressincronize o grupo de consistência:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

Converta um relacionamento SnapMirror existente em ativo-ativo simétrico

A partir do ONTAP 9.15,1, você pode converter uma relação existente do SnapMirror para uma relação ativa/ativa simétrica de sincronização ativa do SnapMirror.

Antes de começar

- Você deve estar executando o ONTAP 9.15,1 ou posterior.
- Uma relação de sincronização com SnapMirror RPO zero deve existir entre o cluster primário e o secundário.
- Todos os LUNs no volume de destino devem ser não mapeados antes que a relação zero rto SnapMirror possa ser criada.
- O SnapMirror active Sync só é compatível com protocolos SAN (não NFS/CIFS). Certifique-se de que nenhum componente do grupo de consistência está montado para acesso nas.

Passos

1. A partir do cluster secundário, execute uma atualização do SnapMirror sobre a relação existente:

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. Verifique se a atualização do SnapMirror foi concluída com êxito:

```
SiteB::>snapmirror show
```

3. Pausar cada um dos relacionamentos síncronos com RPO zero:

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Exclua cada uma das relações síncronas com RPO zero:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Libere a relação de origem do SnapMirror, mas mantenha as cópias Snapshot comuns:

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Crie uma relação síncrona de rto SnapMirror zero com a política AutomatedFailoverDuplex:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. Se os hosts existentes forem locais, o cluster primário, adicione o host ao cluster secundário e estabeleça conetividade com o respetivo acesso a cada cluster.
8. No site secundário, exclua os mapas LUN nos grupos associados aos hosts remotos.

   Certifique-se de que o grupo não contenha mapas para LUNs não replicados.

```
SiteB::> lun mapping delete -vserver svm_name -igroup igroup -path <>
```

9. No local principal, modifique a configuração do iniciador para os hosts existentes para definir o caminho proximal para os iniciadores no cluster local.

```
SiteA::> igroup initiator add-proximal-vserver -vserver svm_name -initiator
host -proximal-vserver server
```

10. Adicione um novo grupo e iniciador para os novos hosts e defina a proximidade do host para a afinidade do host para seu site local. Replicação do igroup para replicar a configuração e inverter a localidade do host no cluster remoto.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. Descubra os caminhos nos hosts e verifique se os hosts têm um caminho Ativo/otimizado para o LUN de armazenamento a partir do cluster preferido
12. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters.
13. Ressincronize o grupo de consistência:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

Converter tipo de relação de sincronização ativa do SnapMirror

A partir do ONTAP 9.15,1, você pode converter entre os tipos de proteção de sincronização ativa SnapMirror: De assimétrica a simétrica ativa ativa/ativa e vice-versa.

Converter em um relacionamento ativo-ativo simétrico

Você pode converter uma relação de sincronização ativa do SnapMirror com a proteção aysnasonic para usar ativo/ativo simétrico.

Antes de começar

- Ambos os clusters devem estar executando o ONTAP 9.15,1 ou posterior.
- Configurações ativo-ativo simétricas exigem a `AutomatedFailoverDuplex` política de proteção. Como alternativa, você pode Crie uma política de SnapMirror personalizada fornecer o `-type` is `automated-failover-duplex`.

System Manager

Passos para uma configuração uniforme

1. Remova o igrop de destino:
   a. No cluster de destino, navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo com o relacionamento SnapMirror e, em seguida, **Excluir**.
   c. Na caixa de diálogo, selecione a caixa **Unmap the Associated LUNs** (Anular mapeamento dos LUNs associados) e **Delete** (Excluir).
2. Edite a relação de sincronização ativa do SnapMirror.
   a. Navegue até **proteção** > **relacionamentos**.
   b. Selecione o menu kabob ao lado do relacionamento que você deseja modificar e, em seguida, **Editar**.
   c. Modifique a **Política de proteção** para AutomatedFailoverDuplex.
   d. A seleção `AutoMatedFailoverDuplex` de solicita uma caixa de diálogo para modificar as configurações de proximidade do host. Para os iniciadores, selecione a opção apropriada para **Iniciador proximal a** e, em seguida, **Guardar**.
   e. Selecione **Guardar**.
3. No menu **proteção**, confirme a operação bem-sucedida quando a relação for exibida como `InSync`.

Passos para uma configuração não uniforme

1. Remova o igrop de destino:
   a. No local secundário, navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo com o relacionamento SnapMirror e, em seguida, **Excluir**.
   c. Na caixa de diálogo, selecione a caixa **Unmap the Associated LUNs** (Anular mapeamento dos LUNs associados) e **Delete** (Excluir).
2. Crie um novo grupo:
   a. No menu **SAN Initiator Groups** no local de destino, selecione **Add**.
   b. Forneça um **Nome**, selecione **sistema operacional anfitrião** e, em seguida, escolha **Membros do Grupo Iniciador**.
   c. Selecione **Guardar**.
3. Mapeie o novo grupo para os LUNs de destino.
   a. Navegue até **armazenamento** > **LUNs**.
   b. Selecione todos os LUNs para mapear para o grupo.
   c. Selecione **More** (mais) e depois **Map to Initiator Groups (mapa para grupos de iniciadores)**.
4. Edite a relação de sincronização ativa do SnapMirror.
   a. Navegue até **proteção** > **relacionamentos**.
   b. Selecione o menu kabob ao lado do relacionamento que você deseja modificar e, em seguida, **Editar**.
   c. Modifique a **Política de proteção** para AutomatedFailoverDuplex.
   d. Selecionar AutoMatedFailoverDuplex inicia a opção para modificar as configurações de proximidade do host. Para os iniciadores, selecione a opção apropriada para **Iniciador proximal**

a e, em seguida, **Guardar**.

e. Selecione **Guardar**.

5. No menu **proteção**, confirme a operação bem-sucedida quando a relação for exibida como `InSync`.

CLI

Passos para uma configuração uniforme

1. Modifique a política SnapMirror de `AutomatedFailover` para `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path destination_path -policy
   AutomatedFailoverDuplex
   ```

2. A modificação da política aciona uma ressincronização. Aguarde até que a ressincronização seja concluída e confirme que a relação é `Insync`:

   ```
   snapmirror show -destination-path destination_path
   ```

3. Se os hosts existentes forem locais, o cluster primário, adicione o host ao segundo cluster e estabeleça conetividade com o respetivo acesso a cada cluster.

4. No site secundário, exclua os mapas LUN nos grupos associados aos hosts remotos.

   Certifique-se de que o grupo não contenha mapas para LUNs não replicados.

   ```
   SiteB::> lun mapping delete -vserver svm_name -igroup igroup -path <>
   ```

5. No local principal, modifique a configuração do iniciador para os hosts existentes para definir o caminho proximal para os iniciadores no cluster local.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver svm_name -initiator
   host -proximal-vserver server
   ```

6. Adicione um novo grupo e iniciador para os novos hosts e defina a proximidade do host para a afinidade do host para seu site local. Replicação do igroup para replicar a configuração e inverter a localidade do host no cluster remoto.

   ```
   SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
   SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
   host2 -proximal-vserver vsB
   ```

7. Descubra os caminhos nos hosts e verifique se os hosts têm um caminho Ativo/otimizado para o LUN de armazenamento a partir do cluster preferido

8. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters.

Passos para uma configuração não uniforme

1. Modifique a política SnapMirror de `AutomatedFailover` para `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path destination_path -policy
   AutomatedFailoverDuplex
   ```

2. A modificação da política aciona uma ressincronização. Aguarde até que a ressincronização seja concluída e confirme que a relação é `Insync`:

   ```
   snapmirror show -destination-path destination_path
   ```

3. Se os hosts existentes forem locais para o cluster primário, adicione o host ao segundo cluster e estabeleça conetividade com o respetivo acesso a cada cluster.
4. No site secundário, exclua os mapas LUN nos grupos associados aos hosts remotos.

   Certifique-se de que o grupo não contenha mapas para LUNs não replicados.

   ```
   SiteB::> lun mapping delete -vserver svm_name -igroup igroup -path <>
   ```

5. No local principal, modifique a configuração do iniciador para os hosts existentes para definir o caminho proximal para os iniciadores no cluster local.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver Svm_name -initiator
   host -proximal-vserver server
   ```

6. No site secundário, adicione um novo grupo e iniciador para os novos hosts e defina a proximidade do host para a afinidade do host para seu site local. Mapeie os LUNs para o grupo.

   ```
   SiteB::> igroup create -vserver svm_name -igroup igroup_name
   SiteB::> igroup add -vserver svm_name -igroup igroup_name -initiator
   host_name
   SiteB::> lun mapping create -igroup igroup_name -path path_name
   ```

7. Descubra os caminhos nos hosts e verifique se os hosts têm um caminho Ativo/otimizado para o LUN de armazenamento a partir do cluster preferido
8. Implante o aplicativo e distribua as cargas de trabalho da VM entre clusters.

Converter de ativo-ativo simétrico para uma relação assimétrica

Se você configurou a proteção ativa/ativa simétrica, você pode converter a relação para proteção assimétrica usando a CLI do ONTAP.

Passos

1. Mova todos os workloads de VM para o host local para o cluster de origem.
2. Remova a configuração do igrop para os hosts que não estão gerenciando as instâncias da VM e modifique a configuração do igrop para encerrar a replicação do igrop.

   ```
   code
   ```

3. No local secundário, desmapeie os LUNs.

   ```
   SiteB::> lun mapping delete -vserver svm_name -igroup igroup_name -path <>
   ```

4. No site secundário, exclua a relação ativo-ativo simétrica.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. No local principal, libere o relacionamento ativo-ativo simétrico.
```
SiteA::> snapmirror release -destination-path destination_path -relationship
-info-only true
```

6. A partir do site secundário, crie uma relação com o mesmo conjunto de volumes com a `AutomatedFailover` política de ressincronizar a relação.

```
SiteB::> snapmirror create -source-path source_path -destination-path
destination_path -cg-item-mappings source:@destination -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst
```

> O grupo de consistência no site secundário precisa "a eliminar" antes de recriar a relação. Os volumes de "Tem de ser convertido para o tipo DP"destino .

7. Confirme se o estado do espelho de relacionamento é `Snapmirrored` o Status do relacionamento é `Insync`.

```
snapmirror show -destination-path destination_path
```

8. Redescubra os caminhos do anfitrião.

Gerencie a sincronização ativa do SnapMirror e proteja os dados

Crie uma cópia Snapshot comum

Além das operações de cópia Snapshot programadas regularmente, você pode criar manualmente um comum "Cópia Snapshot" entre os volumes no grupo de consistência do SnapMirror primário e os volumes no grupo de consistência do SnapMirror secundário.

Sobre esta tarefa

O intervalo de criação de Snapshot programado é de 12 horas.

Antes de começar

- A relação de grupo SnapMirror deve estar sincronizada.

Passos

1. Criar uma cópia Snapshot comum:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Monitorize o progresso da atualização:

```
destination::>snapmirror show -fields -newest-snapshot
```

Executar um failover planejado de clusters em uma relação de sincronização ativa do SnapMirror

Em um failover planejado de clusters do ONTAP em uma relação de sincronização ativa do SnapMirror, você alterna as funções dos clusters primário e secundário para que o cluster secundário assuma o controle do cluster primário. Durante um failover, o que normalmente é o cluster secundário processa as solicitações de entrada e saída localmente sem interromper as operações do cliente.

Você pode querer executar um failover planejado para testar a integridade da configuração de recuperação de desastres ou para executar a manutenção no cluster primário.

Sobre esta tarefa

Um failover planejado é iniciado pelo administrador do cluster secundário. A operação requer a comutação das funções primária e secundária para que o cluster secundário assuma o controle do primário. O novo cluster primário pode então começar a processar solicitações de entrada e saída localmente sem interromper as operações do cliente.

Antes de começar

- A relação de sincronização ativa do SnapMirror deve estar sincronizada.
- Não é possível iniciar um failover planejado quando uma operação sem interrupções está em processo. As operações ininterruptas incluem movimentação de volume, realocação de agregados e failovers de storage.
- O Mediador ONTAP deve ser configurado, conetado e no quórum.

Passos

Você pode executar um failover planejado usando a CLI do ONTAP ou o Gerenciador de sistema.

System Manager

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

1. No System Manager, selecione **proteção > Visão geral > relacionamentos**.
2. Identifique a relação de sincronização ativa do SnapMirror que você deseja fazer failover. Ao lado de seu nome, selecione o … próximo ao nome do relacionamento e, em seguida, selecione **failover**.
3. Para monitorar o status do failover, use o `snapmirror failover show` na CLI do ONTAP.

CLI

1. A partir do cluster de destino, inicie a operação de failover:

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Monitore o progresso do failover:

   ```
   destination::>snapmirror failover show
   ```

3. Quando a operação de failover estiver concluída, você poderá monitorar o status do relacionamento de proteção síncrona SnapMirror a partir do destino:

   ```
   destination::>snapmirror show
   ```

Recuperar de operações automáticas de failover não planejadas

Uma operação automática de failover não planejado (AUFO) ocorre quando o cluster primário está inativo ou isolado. O Mediador ONTAP deteta quando ocorre um failover e executa um failover automático não planejado para o cluster secundário. O cluster secundário é convertido para o primário e começa a servir os clientes. Esta operação é realizada apenas com a ajuda do Mediador ONTAP.

Após o failover automático não planejado, é importante reexaminar os caminhos de e/S LUN do host para que não haja perda de caminhos de e/S.

Restabeleça o relacionamento de proteção após um failover não planejado

É possível restabelecer a relação de proteção usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

Passos

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

1. Navegue até **proteção > relacionamentos** e aguarde que o estado da relação mostre "InSync".
2. Para retomar as operações no cluster de origem original, clique ⋮ e selecione **failover**.

CLI

Você pode monitorar o status do failover automático não planejado usando o `snapmirror failover show` comando.

Por exemplo:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte "Referência da EMS"para obter informações sobre mensagens de eventos e sobre ações corretivas.

Retomar a proteção em uma configuração de fan-out após o failover

A partir do ONTAP 9.15,1, o SnapMirror ative Sync suporta reconfiguração automática na etapa fan-out após um evento de failover. Para obter mais informações, "configurações de fan-out"consulte .

Se você estiver usando o ONTAP 9.14,1 ou anterior e tiver um failover no cluster secundário na relação de sincronização ativa do SnapMirror, o destino assíncrono do SnapMirror não será saudável. Você deve restaurar manualmente a proteção excluindo e recriando a relação com o endpoint assíncrono do SnapMirror.

Passos

1. Verifique se o failover foi concluído com êxito:
   `snapmirror failover show`
2. No endpoint assíncrono do SnapMirror, exclua o endpoint de fan-out:
   `snapmirror delete -destination-path` *`destination_path`*
3. No terceiro site, crie relações assíncronas do SnapMirror entre o novo volume primário de sincronização ativa do SnapMirror e o volume de destino de saída de ventoinha assíncrona:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`*

`-policy MirrorAllSnapshots -schedule schedule`

4. Ressincronizar a relação:
`snapmirror resync -destination-path destination_path`
5. Verifique o status e a saúde da relação:
`snapmirror show`

Monitorar operações de sincronização ativa do SnapMirror

Você pode monitorar as seguintes operações de sincronização ativa do SnapMirror para garantir a integridade da configuração de sincronização ativa do SnapMirror:

- ONTAP Mediador
- Operações de failover planejadas
- Operações automáticas de failover não planejadas
- Disponibilidade de sincronização ativa do SnapMirror

> A partir do ONTAP 9.15,1, o Gerenciador do sistema exibe o status da relação de sincronização ativa do SnapMirror de qualquer cluster. Você também pode monitorar o status do Mediador ONTAP de qualquer cluster no Gerenciador de sistema.

ONTAP Mediador

Durante as operações normais, o estado do Mediador ONTAP deve ser conetado. Se estiver em qualquer outro estado, isso pode indicar uma condição de erro. Pode rever o "Mensagens do sistema de Gestão de Eventos (EMS)" para determinar o erro e as ações corretivas adequadas.

Operações de failover planejadas

Você pode monitorar o status e o progresso de uma operação de failover planejada usando o `snapmirror failover show` comando. Por exemplo:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Depois que a operação de failover estiver concluída, você poderá monitorar o status de proteção SnapMirror a partir do novo cluster de destino. Por exemplo:

```
ClusterA::> snapmirror show
```

Consulte "Referência da EMS"para obter informações sobre mensagens de eventos e ações corretivas.

Operações automáticas de failover não planejadas

Durante um failover automático não planejado, você pode monitorar o status da operação usando o `snapmirror failover show` comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte "Referência da EMS"para obter informações sobre mensagens de eventos e sobre ações corretivas.

Disponibilidade de sincronização ativa do SnapMirror

Você pode verificar a disponibilidade da relação de sincronização ativa do SnapMirror usando uma série de comandos, no cluster primário, no cluster secundário ou em ambos.

Os comandos usados incluem o `snapmirror mediator show` comando no cluster primário e secundário para verificar o status da conexão e do quórum, o `snapmirror show` comando e o `volume show` comando. Por exemplo:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

Adicione ou remova volumes a um grupo de consistência

À medida que os requisitos de workload do aplicativo mudam, você pode precisar adicionar ou remover volumes de um grupo de consistência para garantir a continuidade dos negócios. O processo de adição e remoção de volumes em uma relação de sincronização ativa do SnapMirror depende da versão do ONTAP que você está usando.

Na maioria dos casos, este é um processo disruptivo que exige que você exclua a relação SnapMirror, modifique o grupo de consistência e, em seguida, retome a proteção. A partir do ONTAP 9.13,1, adicionar volumes a um grupo de consistência com uma relação SnapMirror ativa é uma operação sem interrupções.

Sobre esta tarefa

- No ONTAP 9.9,1, você pode adicionar ou remover volumes a um grupo de consistência usando a CLI do ONTAP.
- A partir do ONTAP 9.10,1, é recomendável que você gerencie "grupos de consistência" por meio do Gerenciador de sistema ou com a API REST do ONTAP.

  Se você quiser alterar a composição do grupo de consistência adicionando ou removendo um volume, primeiro exclua a relação original e, em seguida, crie o grupo de consistência novamente com a nova composição.

- A partir do ONTAP 9.13,1, você pode adicionar volumes a um grupo de consistência sem interrupções com uma relação do SnapMirror ativa da origem ou destino.

  Remover volumes é uma operação disruptiva. Você deve excluir a relação do SnapMirror antes de remover volumes.

ONTAP 9.9,1-9.13.0

Antes de começar

- Você não pode começar a modificar o grupo de consistência enquanto ele estiver no `InSync` estado.
- O volume de destino deve ser do tipo DP.
- O novo volume adicionado para expandir o grupo de consistência precisa ter um par de cópias Snapshot comuns entre os volumes de origem e destino.

Passos

Os exemplos mostrados em dois mapeamentos de volume: `vol_src1 vol_dst1 vol_src2 vol_dst2` Em uma relação de grupo de consistência entre os pontos finais `vs1_src:/cg/cg_src` e `vs1_dst:/cg/cg_dst`.

1. Nos clusters de origem e destino, verifique se há um Snapshot comum entre os clusters de origem e destino com o comando `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. Se não existir uma cópia Snapshot comum, crie e inicialize uma relação FlexVol SnapMirror:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Excluir a relação do grupo de consistência:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
   ```

4. Solte a relação de origem do SnapMirror e mantenha as cópias Snapshot comuns:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Desmapeie os LUNs e exclua a relação de grupo de consistência existente:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > Os LUNs de destino não são mapeados, enquanto os LUNs na cópia primária continuam a servir a e/S do host

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **Se você estiver usando ONTAP 9.10,1 até 9.13.0,** delete e recrie e o grupo consistência na fonte

com a composição correta. Siga os passos em Excluir um grupo de consistência e, Configurar um único grupo de consistênciaem seguida, . No ONTAP 9.10,1 e posterior, você deve executar as operações de exclusão e criação no Gerenciador de sistema ou com a API REST do ONTAP; não há procedimento de CLI.

Se você estiver usando o ONTAP 9.9,1, vá para a próxima etapa.

7. Crie o novo grupo de consistência no destino com a nova composição:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Ressincronize a relação do grupo de consistência rto zero para garantir que ela esteja sincronizada:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Remapear os LUNs não mapeados na Etapa 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

ONTAP 9.13,1 e posterior

A partir do ONTAP 9.13,1, você pode adicionar volumes a um grupo de consistência sem interrupções com uma relação de sincronização ativa do SnapMirror. O SnapMirror ative Sync suporta a adição de volumes da origem ou do destino.

> Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

Para obter detalhes sobre como adicionar volumes do grupo de consistência de origem, Modifique um grupo de consistênciaconsulte .

Adicione um volume do cluster de destino

1. No cluster de destino, selecione **proteção** > **relacionamentos**.
2. Encontre a configuração do SnapMirror à qual deseja adicionar volumes. Selecione ⋮ e, em seguida, **expandir**.
3. Selecione as relações de volume cujos volumes devem ser adicionados ao grupo de consistência
4. Selecione **expandir**.

Atualize e reverta o ONTAP com a sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror é suportada a partir do ONTAP 9.9,1. A atualização e reversão do cluster do ONTAP tem implicações nas relações de sincronização ativa do SnapMirror, dependendo da versão do ONTAP para a qual você está atualizando ou revertendo.

Atualize o ONTAP com a sincronização ativa do SnapMirror

Para usar a sincronização ativa do SnapMirror, todos os nós nos clusters de origem e destino devem estar executando o ONTAP 9.9,1 ou posterior.

Ao atualizar o ONTAP com relações de sincronização ativas do SnapMirror, você deve usar Atualização automatizada sem interrupções (ANDU)o . O uso DO ANDU garante que suas relações de sincronização ativa do SnapMirror estejam sincronizadas e íntegras durante o processo de atualização.

Não há etapas de configuração para preparar implantações de sincronização ativa do SnapMirror para atualizações do ONTAP. No entanto, é recomendável que antes e depois da atualização, você verifique se:

- As relações de sincronização ativa do SnapMirror estão sincronizadas.
- Não existem erros relacionados ao SnapMirror no registo de eventos.
- O Mediator está on-line e saudável de ambos os clusters.
- Todos os hosts podem ver todos os caminhos corretamente para proteger LUNs.

> Quando você atualiza clusters do ONTAP 9.9,1 ou 9.9.1 para o ONTAP 9.10,1 e posterior, o ONTAP cria novos grupos de consistênciaclusters de origem e destino para as relações de sincronização ativa do SnapMirror que podem ser configuradas usando o Gerenciador do sistema.

> `snapmirror quiesce`Os comandos e `snampirror resume` não são suportados com a sincronização ativa do SnapMirror.

Reverter para ONTAP 9.9,1 a partir de ONTAP 9.10,1

Para reverter relacionamentos de 9.10.1 para 9,9.1, as relações de sincronização ativa do SnapMirror devem ser excluídas, seguidas pela instância do grupo de consistência do 9.10.1. Os grupos de consistência com uma relação de sincronização ativa do SnapMirror não podem ser excluídos. Todos os volumes do FlexVol que foram atualizados para o 9.10.1 anteriormente associados a outro contêiner inteligente ou aplicativo empresarial em 9.9.1 ou anterior não serão mais associados ao Revert. A exclusão de grupos de consistência não exclui os volumes constituintes ou instantâneos granulares de volume. "Excluir um grupo de consistência"Consulte para obter mais informações sobre esta tarefa no ONTAP 9.10,1 e posterior.

Reverter de ONTAP 9.9,1

> A sincronização ativa do SnapMirror não é compatível com clusters ONTAP mistos do que incluir versões anteriores ao ONTAP 9.9,1.

Ao reverter do ONTAP 9.9,1 para uma versão anterior do ONTAP, você deve estar ciente do seguinte:

- Se o cluster hospedar um destino de sincronização ativa do SnapMirror, reverter para o ONTAP 9.8 ou anterior não será permitido até que o relacionamento seja quebrado e excluído.
- Se o cluster hospedar uma fonte de sincronização ativa do SnapMirror, reverter para o ONTAP 9.8 ou anterior não será permitido até que a relação seja liberada.
- Todas as políticas de sincronização ativa do SnapMirror personalizadas criadas pelo usuário devem ser excluídas antes de reverter para o ONTAP 9.8 ou anterior.

Para atender a esses requisitos, "Remova uma configuração de sincronização ativa do SnapMirror"consulte .

Passos

1. Confirme sua prontidão para reverter, inserindo o seguinte comando de um dos clusters na relação de sincronização ativa do SnapMirror:

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   A saída de amostra a seguir mostra um cluster que não está pronto para reverter com instruções para limpeza.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
      abort
       Command to see if the Relationship Status of a SnapMirror
   relationship
      is Quiesced: snapmirror show
       Command to break off a data-protection volume: snapmirror break
       Command to break off a data-protection volume which is the
   destination
      of a SnapMirror relationship with a policy of type "vault":
   snapmirror
      break -delete-snapshots
   ```

```
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. Depois de atender aos requisitos da verificação Reverter, "Reverter ONTAP"consulte .

Remova uma configuração de sincronização ativa do SnapMirror

Se você não precisar mais de proteção síncrona de rto SnapMirror zero, poderá excluir sua relação de sincronização ativa do SnapMirror.

Remova uma configuração assimétrica

- Antes de excluir a relação de sincronização ativa do SnapMirror, todos os LUNs no cluster de destino devem ser não mapeados.
- Depois que os LUNs não são mapeados e o host é reconfigurado, o destino SCSI notifica os hosts de que o inventário LUN foi alterado. Os LUNs existentes nos volumes secundários de rto zero mudam para refletir uma nova identidade depois que a relação rto zero é excluída. Os hosts descobrem os LUNs de volume secundário como novos LUNs que não têm relação com os LUNs de volume de origem.
- Os volumes secundários permanecem volumes DP depois que a relação é excluída. Você pode emitir o `snapmirror break` comando para convertê-los para ler/escrever.
- A exclusão do relacionamento não é permitida no estado de failover quando o relacionamento não é revertido.

Passos

1. No cluster secundário, remova a relação do grupo de consistência de sincronização ativa do SnapMirror entre o ponto final de origem e o ponto de extremidade de destino:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. No cluster primário, solte a relação de grupo de consistência e as cópias Snapshot criadas para a relação:

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Execute uma nova verificação do host para atualizar o inventário LUN.
4. A partir do ONTAP 9.10,1, a exclusão da relação SnapMirror não exclui o grupo de consistência. Se você quiser excluir o grupo de consistência, use o Gerenciador do sistema ou a API REST do ONTAP. Consulte Excluir um grupo de consistência para obter mais informações.

Remover uma configuração ativo-ativo simétrica

Você pode remover uma configuração simétrica usando o Gerenciador do sistema ou a CLI do ONTAP. Em ambas as interfaces, existem diferentes etapas para configurações uniformes e não uniformes.

System Manager

Passos para uma configuração uniforme

1. No site principal, remova os hosts remotos do igrop e encerre a replicação.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo que você deseja modificar e, em seguida, **Editar**.
   c. Remova o iniciador remoto e encerre a replicação do igroup. Selecione **Guardar**.
2. No site secundário, exclua a relação replicada desmapeando os LUNs.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo com o relacionamento SnapMirror e, em seguida, **Excluir**.
   c. Na caixa de diálogo, selecione a caixa **Unmap the Associated LUNs** (Anular mapeamento dos LUNs associados) e **Delete** (Excluir).
   d. Navegue até **proteção** > **relacionamentos**.
   e. Selecione a relação de sincronização ativa do SnapMirror e, em seguida, **Liberação** para excluir as relações.

Passos para uma configuração não uniforme

1. No site principal, remova os hosts remotos do igrop e encerre a replicação.
   a. Navegue até **hosts** > **grupos de iniciadores SAN**.
   b. Selecione o grupo que você deseja modificar e, em seguida, **Editar**.
   c. Remova o iniciador remoto e encerre a replicação do igroup. Selecione **Guardar**.
2. No local secundário, remova a relação de sincronização ativa do SnapMirror.
   a. Navegue até **proteção** > **relacionamentos**.
   b. Selecione a relação de sincronização ativa do SnapMirror e, em seguida, **Liberação** para excluir as relações.

CLI

Passos para uma configuração uniforme

1. Mova todos os workloads de VM para o host local para o cluster de origem da sincronização ativa do SnapMirror.
2. No cluster de origem, remova os iniciadores do iggroup e modifique a configuração do iggroup para encerrar a replicação do iggroup.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. No site secundário, exclua o mapeamento de LUN e remova a configuração do igroup:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. No site secundário, exclua a relação de sincronização ativa do SnapMirror.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. No local principal, libere a relação de sincronização ativa do SnapMirror do local principal.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Redescubra os caminhos para verificar se apenas o caminho local está disponível para o host.

Passos para uma configuração não uniforme

1. Mova todos os workloads de VM para o host local para o cluster de origem da sincronização ativa do SnapMirror.
2. No cluster de origem, remova os iniciadores do igrop.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. No site secundário, exclua o mapeamento de LUN e remova a configuração do igroup:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. No site secundário, exclua a relação de sincronização ativa do SnapMirror.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. No local principal, libere a relação de sincronização ativa do SnapMirror do local principal.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Redescubra os caminhos para verificar se apenas o caminho local está disponível para o host.

Remova o Mediador ONTAP

Se você quiser remover uma configuração existente do ONTAP Mediator dos clusters do ONTAP, use o `snapmirror mediator remove` comando.

Passos

1. Remover o Mediador ONTAP:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
cluster_xyz
```

Solucionar problemas

A operação de exclusão do SnapMirror falha no estado takover

Problema:

Quando o ONTAP 9.9,1 é instalado em um cluster, a execução do `snapmirror delete` comando falha quando uma relação de grupo de consistência de sincronização

ativa do SnapMirror está no estado de aquisição.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solução

Quando os nós de uma relação de sincronização ativa do SnapMirror estiverem no estado de aquisição, execute a operação de exclusão e liberação do SnapMirror com a opção "-force" definida como verdadeiro.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Falha ao criar uma relação SnapMirror e inicializar um grupo de consistência

Problema:

Falha na criação da relação e inicialização do grupo de consistência do SnapMirror.

Solução:

Certifique-se de que não excedeu o limite de grupos de consistência por cluster. Os limites do grupo de consistência na sincronização ativa do SnapMirror são independentes da plataforma e diferem com base na versão do ONTAP. Consulte "Limites de objetos" para obter orientações específicas para a sua versão do ONTAP.

Erro:

Se o grupo de consistência estiver bloqueado na inicialização, verifique o status das inicializações do grupo de consistência com a API REST do ONTAP, o Gerenciador de sistema ou o comando `sn show -expand`.

Do ONTAP 9.8 ao 9.14.1, a sincronização ativa do SnapMirror é chamada de continuidade de negócios do SnapMirror (SM-BC).

Solução:

Se os grupos de consistência não iniciarem, remova a relação de sincronização ativa do SnapMirror, exclua o grupo de consistência e, em seguida, recrie a relação e inicialize-a. Este fluxo de trabalho difere dependendo da versão do ONTAP que você está usando.

Se estiver a utilizar o ONTAP 9.9,1	Se estiver a utilizar o ONTAP 9.10,1 ou posterior

1. "Remova a configuração de sincronização ativa do SnapMirror" 2. "Crie uma relação de grupo de consistência e, em seguida, inicialize a relação de grupo de consistência"	1. Em **proteção > relacionamentos**, encontre a relação de sincronização ativa do SnapMirror no grupo consistência. Selecione e, em seguida, **Excluir** para remover a relação de sincronização ativa do SnapMirror. 2. "Exclua o grupo de consistência" 3. "Configure o grupo de consistência"

Failover planejado sem êxito

Problema:

Depois de executar o `snapmirror failover start` comando, a saída para o `snapmirror failover show` comando exibe uma mensagem indica que uma operação sem interrupções está em andamento.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                          08:35:04
08:35:04
```

Causa:

Um failover planejado não pode começar quando uma operação sem interrupções estiver em andamento, incluindo movimentação de volume, realocação de agregado e failover de storage.

Solução:

Aguarde até que a operação sem interrupções seja concluída e tente a operação de failover novamente.

O status do quórum do mediador ONTAP não é alcançável ou falso

Problema:

Depois de executar o `snapmirror failover start` comando, a saída para `snapmirror failover show` o comando exibe uma mensagem indicando que o Mediador ONTAP não está configurado.

"Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Causa:

O mediador não está configurado ou há problemas de conetividade de rede.

Solução:

Se o Mediador do ONTAP não estiver configurado, você deverá configurar o Mediador do ONTAP antes de estabelecer uma relação de sincronização ativa do SnapMirror. Corrija quaisquer problemas de conetividade de rede. Certifique-se de que o Mediador esteja conetado e o status do quórum seja verdadeiro no local de origem e destino usando o comando SnapMirror Mediator show. Para obter mais informações, "Configure o Mediador ONTAP"consulte .

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Failover não planejado automático não acionado no local B.

Problema:

Uma falha no local A não aciona um failover não planejado no local B..

Causa possível n.o 1:

O Mediador ONTAP não está configurado. Para determinar se esta é a causa, emita o `snapmirror mediator show` comando no cluster do local B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Este exemplo indica que o Mediador ONTAP não está configurado no local B.

Solução:

Certifique-se de que o ONTAP Mediator esteja configurado em ambos os clusters, de que o status esteja conetado e de que o quórum esteja definido como verdadeiro.

Causa possível n.o 2:

O grupo de consistência do SnapMirror está fora de sincronia. Para determinar se essa é a causa, exiba o log de eventos para ver se o grupo de consistência estava em sincronia durante o momento em que ocorreu a

falha do Site A.

```
cluster::*> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solução:

Conclua as etapas a seguir para executar um failover forçado no local B.

1. Desmapear todos os LUNs pertencentes ao grupo de consistência do Site B..
2. Exclua a relação do grupo de consistência do SnapMirror usando a `force` opção.
3. Digite o `snapmirror break` comando nos volumes constituintes do grupo de consistência para converter volumes de DP para R/W, para habilitar e/S do local B.
4. Inicialize os nós do local A para criar uma relação rto zero do local B para o local A..
5. Libere o grupo de consistência com `relationship-info-only` o no local A para reter a cópia Snapshot comum e desmapear os LUNs pertencentes ao grupo de consistência.
6. Converta volumes no local A de R/W para DP configurando uma relação de nível de volume usando a política de sincronização ou a política de sincronização.
7. Emita o `snapmirror resync` para sincronizar as relações.
8. Exclua os relacionamentos do SnapMirror com a política de sincronização no local A..
9. Liberar as relações SnapMirror com a política de sincronização usando `relationship-info-only true` no local B..
10. Crie uma relação de grupo de consistência do local B para o local A..
11. Execute uma ressincronização do grupo de consistência no Site A e verifique se o grupo de consistência está em sincronia.
12. Pode novamente hospedar caminhos de e/S LUN para restaurar todos os caminhos para os LUNs.

Link entre o Site B e o Mediator Down e o Site A Down

Para verificar a conexão do Mediador ONTAP, use o `snapmirror mediator show` comando. Se o status da conexão for inalcançável e o local B não conseguir alcançar o local A, você terá uma saída semelhante à abaixo. Siga as etapas da solução para restaurar a conexão

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solução

Forçar um failover para habilitar a e/S do local B e, em seguida, estabelecer uma relação rto zero do local B para o local A. conclua as etapas a seguir para executar um failover forçado no local B.

1. Desmapear todos os LUNs pertencentes ao grupo de consistência do Site B..
2. Exclua a relação do grupo de consistência do SnapMirror usando a opção forçar.
3. Digite o comando SnapMirror Break (`snapmirror break -destination_path` *svm*`:_volume_`) nos volumes constituintes do grupo de consistência para converter volumes de DP para RW, para ativar e/S do local B.

   Você deve emitir o comando SnapMirror Break para cada relacionamento no grupo consistência. Por exemplo, se houver três volumes no grupo consistência, você emitirá o comando para cada volume.

4. Inicialize os nós do local A para criar uma relação rto zero do local B para o local A..

5. Libere o grupo de consistência com somente informações de relacionamento no Site A para reter a cópia Snapshot comum e desmapear os LUNs pertencentes ao grupo de consistência.
6. Converta volumes no local A de RW para DP configurando uma relação de nível de volume usando a política de sincronização ou a política de sincronização.
7. Emita o `snapmirror resync` comando para sincronizar as relações.
8. Excluir as relações SnapMirror com a política de sincronização no local A..
9. Libere as relações do SnapMirror com a política de sincronização usando somente relacionamento verdadeiro no local B..
10. Crie uma relação de grupo de consistência entre o local B e o local A..
11. No cluster de origem, ressincronize o grupo de consistência. Verifique se o estado do grupo de consistência está em sincronia.
12. Reescaneie os caminhos de e/S LUN do host para restaurar todos os caminhos para os LUNs.

Ligação entre o Site A e o Mediator Down e o Site B Down

Ao usar a sincronização ativa do SnapMirror, você pode perder a conetividade entre o Mediador do ONTAP ou seus clusters com peering. É possível diagnosticar o problema verificando o status de conexão, disponibilidade e consenso das diferentes partes da relação de sincronização ativa do SnapMirror e, em seguida, retomando a conexão com força.

O que verificar	Comando CLI	Indicador
Mediador do Site A	`snapmirror mediator show`	O estado da ligação é apresentado como `unreachable`
Conetividade do local B.	`cluster peer show`	A disponibilidade é apresentada como `unavailable`
Status de consenso do volume de sincronização ativa do SnapMirror	`volume show` *`volume_name`* `-fields smbc-consensus`	O `sm-bc consensus` campo é exibido `Awaiting-consensus`

Para obter informações adicionais sobre como diagnosticar e resolver este problema, consulte o artigo da base de dados de Conhecimento "Ligação entre o local A e o Mediador para baixo e o local B para baixo ao utilizar a sincronização ativa do SnapMirror".

A operação de exclusão do SnapMirror falha quando a vedação está definida no volume de destino

Problema:

A operação de exclusão do SnapMirror falha quando qualquer um dos volumes de destino tiver uma vedação de redirecionamento definida.

Solução

Executar as seguintes operações para tentar novamente o redirecionamento e remover a cerca do volume de destino.

- Ressincronização do SnapMirror
- Atualização do SnapMirror

Operação de movimentação de volume emperrada quando o primário está para baixo

Problema:

Uma operação de movimentação de volume fica presa indefinidamente no estado de transição adiada quando o local principal está inativo em uma relação de sincronização ativa do SnapMirror. Quando o local principal está inativo, o local secundário executa um failover não planejado automático (AUFO). Quando uma operação de movimentação de volume está em andamento quando o AUFO é acionado, o movimento de volume fica preso.

Solução:

Abortar a instância de movimentação de volume que está emperrada e reiniciar a operação de movimentação de volume.

A versão do SnapMirror falha quando não é possível excluir a cópia Snapshot

Problema:

A operação de lançamento do SnapMirror falha quando a cópia Snapshot não pode ser excluída.

Solução:

A cópia Snapshot contém uma tag transitória. Use o `snapshot delete` comando com a `-ignore-owners` opção para remover a cópia Snapshot transitória.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Tente novamente o `snapmirror release` comando.

Referência de movimentação de volume a cópia Snapshot é exibida como a mais recente

Problema:

Depois de executar uma operação de movimentação de volume em um volume de grupo de consistência, a cópia Snapshot de referência de movimentação de volume pode ser exibida incorretamente como a mais recente para a relação SnapMirror.

Você pode exibir a cópia Snapshot mais recente com o seguinte comando:

```
snapmirror show -fields newest-snapshot status -expand
```

Solução:

Execute manualmente uma `snapmirror resync` operação de ressincronização automática seguinte após a conclusão da operação de movimentação de volume.

Serviço de mediador para sincronização ativa do MetroCluster e do SnapMirror

Visão geral do Mediador ONTAP

O Mediador ONTAP fornece várias funções para os recursos do ONTAP:

- Fornece um armazenamento persistente e vedado para metadados de HA.
- Serve como um proxy ping para vivacidade do controlador.
- Fornece funcionalidade de consulta de integridade do nó síncrono para auxiliar na determinação do quórum.

O Mediador ONTAP fornece dois serviços adicionais de systemctl:

- **`ontap_mediator.service`**

  Mantém o servidor REST APIs para gerenciar as relações ONAP.

- **`mediator-scst.service`**

  Controla o arranque e o encerramento do módulo iSCSI (SCST).

Ferramentas fornecidas para o administrador do sistema

Ferramentas fornecidas para o administrador do sistema:

- **`/usr/local/bin/mediator_change_password`**

  Define uma nova senha da API quando o nome de usuário e a senha atuais da API são fornecidos.

- **`/usr/local/bin/mediator_change_user`**

  Define um novo nome de usuário da API quando o nome de usuário e a senha atuais da API são fornecidos.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Gera um arquivo tgz local contendo todas as informações úteis de suporte necessárias para a comunicação com o suporte ao cliente NetApp. Isso inclui configuração de aplicativos, logs e algumas informações do sistema. Os pacotes são gerados no disco local e podem ser transferidos manualmente, conforme necessário. Local de armazenamento: /Opt/NetApp/data/support_bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Remove o pacote do Mediador ONTAP e o módulo do kernel SCST. Isso inclui todas as configurações, Registros e dados de caixa de correio.

- **`/usr/local/bin/mediator_unlock_user`**

  Libera um bloqueio na conta de usuário da API se o limite de tentativas de autenticação foi atingido. Este recurso é usado para evitar a derivação de senha de força bruta. Ele solicita ao usuário o nome de usuário e a senha corretos.

- **`/usr/local/bin/mediator_add_user`**

  (Suporte somente) usado para adicionar o usuário da API após a instalação.

Notas especiais

O Mediador ONTAP depende do SCST para fornecer iSCSI (http://scst.sourceforge.net/index.htmlconsulte). Este pacote é um módulo do kernel que é compilado durante a instalação especificamente para o kernel. Qualquer atualização do kernel pode exigir que o SCST seja reinstalado. Alternativamente, desinstale e reinstale o Mediador ONTAP e, em seguida, reconfigure a relação ONTAP.

> Todas as atualizações do kernel do sistema operacional do servidor devem ser coordenadas com uma janela de manutenção no ONTAP.

O que há de novo com o Mediador ONTAP

Novas melhorias para o Mediador ONTAP são fornecidas com cada versão. Eis as novidades.

Melhorias

Para obter informações sobre a versão do SCST, consulte Matriz de suporte SCST.

ONTAP versão mediadora	Melhorias
1,9	• Suporte para RHEL: ◦ Compatível: 8,4, 8,5, 8,6, 8,7, 8,9, 9,1 e 9,3. ◦ Recomendado: 8,8, 8,10, 9,0, 9,2, 9,4 e 9,5. • Suporte para Rocky Linux 8 e 9. • Suporte FIPS para RHEL e Rocky Linux. • Melhorias de desempenho adicionadas para maior escalabilidade. • Nomes de arquivo aprimorados para simplificar a configuração de certificados assinados pela PKI.
1,8	• Suporte para RHEL 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4. • Suporte para Rocky Linux 8 e 9.
1,7	• Suporte para RHEL 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3. • Suporte para Rocky Linux 8 e 9. • Suporte para dados SAN (Nome alternativo do assunto) em certificados autoassinados e certificados assinados por terceiros.
1,6	• Atualizações do Python 3,9. • Suporte para RHEL 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1 e 9,2. • Suporte para Rocky Linux 8 e 9. • Suporte descontinuado para RHEL 7.x / CentOS todas as versões.

1,5	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9. • Inclui avisos de depreciação para RHEL 7.x / CentOS 7.x. • Otimiza a velocidade para sistemas de sincronização ativos SnapMirror de maior escala. • Assinatura de código criptográfico adicionada ao instalador.
1,4	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9. • Adicionado suporte para o Secure Boot (SB) de firmware baseado em UFEI.
1,3	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9.
1,2	• Suporte para RHEL 7,6, 7,7, 7,8, 7,9, 8,0, 8,1. • Suporte para CentOS 7,6, 7,7, 7,8, 7,9. • Suporte para caixas de correio HTTPS. • Para uso com ONTAP 9.8z AUSO MCC-IP e SnapMirror ative Sync Zrto.
1,1	• Suporte para RHEL 7,6 e 8,0. • Suporte para CentOS 7,6. • Elimina dependências Perl.
1,0	• Suporte para caixas de correio iSCSI. • Para uso com AUSO de MCC-IP ONTAP 9.7. • Suporte para RHEL/CentOS 7,6.

Matriz de suporte de SO

SO para Mediador ONTAP	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
7,6	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Sim	Sim (apenas RHEL)
7,7	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Não	Não
7,8	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Não	Não

7,9	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Compatível	Não	Não
RHEL 8,0	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Sim	Não
RHEL 8,1	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Sim	Não	Não
RHEL 8,2	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Não	Não	Não
RHEL 8,3	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sim	Sim	Sim	Não	Não	Não
RHEL 8,4	Compatível	Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Não
RHEL 8,5	Compatível	Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Não
RHEL 8,6	Compatível	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 8,7	Compatível	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 8,8	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 8,9	Compatível	Sim	Sim	Não	Não	Não	Não	Não	Não	Não
RHEL 8,10	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
RHEL 9,0	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 9,1	Compatível	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 9,2	Sim	Sim	Sim	Sim	Não	Não	Não	Não	Não	Não
RHEL 9,3	Compatível	Sim	Sim	Não	Não	Não	Não	Não	Não	Não

RHEL 9,4	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
RHEL 9,5	Sim	Não	Não	Não	Não	Não	Não	Não	Não	Não
CentOS 8 e stream	Não	Não	Não	Não	Não	Não	Não	N/A.	N/A.	N/A.
Rocky Linux 8	Sim	Sim	Sim	Sim	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.
Rocky Linux 9	Sim	Sim	Sim	Sim	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.

- OS refere-se a versões RedHat e CentOS, a menos que especificado de outra forma.
- "Sim" significa que o SO é recomendado para a instalação do Mediador ONTAP e é totalmente compatível e suportado.
- "Não" significa que o SO e o Mediador ONTAP não são compatíveis.
- "Compatível" significa que o RHEL não suporta mais esta versão, mas o Mediador ONTAP ainda pode ser instalado.
- O CentOS 8 foi removido para todas as versões devido à sua ramificação. O CentOS Stream foi considerado como um sistema operacional de destino de produção adequado. Nenhum suporte está planejado.
- O ONTAP Mediator 1,5 foi a última versão suportada para sistemas operacionais de ramificação RHEL 7.x.
- O ONTAP Mediator 1,6 adiciona suporte para Linux 8 e 9.

Matriz de suporte SCST

A tabela a seguir mostra a versão SCST suportada para cada versão do ONTAP Mediator.

ONTAP versão mediadora	Versão SCST suportada
ONTAP Mediador 1,9	scst-3,8.0.tar.bz2
ONTAP Mediador 1,8	scst-3,8.0.tar.bz2
ONTAP Mediador 1,7	scst-3,7.0.tar.bz2
ONTAP Mediador 1,6	scst-3,7.0.tar.bz2
ONTAP Mediador 1,5	scst-3,6.0.tar.bz2
ONTAP Mediador 1,4	scst-3,6.0.tar.bz2
ONTAP Mediador 1,3	scst-3,5.0.tar.bz2
ONTAP Mediador 1,2	scst-3,4.0.tar.bz2
ONTAP Mediador 1,1	scst-3,4.0.tar.bz2

ONTAP versão mediadora	Versão SCST suportada
ONTAP Mediador 1,0	scst-3,3.0.tar.bz2

Instalar ou atualizar

Prepare-se para instalar ou atualizar o serviço do Mediador ONTAP

Para instalar o serviço ONTAP Mediator, você deve garantir que todos os pré-requisitos sejam atendidos, buscar o pacote de instalação e executar o instalador no host. Este procedimento é utilizado para uma instalação ou atualização de uma instalação existente.

- A partir do ONTAP 9.7, você pode usar qualquer versão do Mediador ONTAP para monitorar uma configuração IP do MetroCluster.
- A partir do ONTAP 9.8, você pode usar qualquer versão do ONTAP Mediator para monitorar uma relação de sincronização ativa do SnapMirror.

Considerações sobre instalação e atualização

Reveja as seguintes considerações antes de atualizar ou instalar o Mediador ONTAP.

> O ONTAP Mediator 1,8 e versões anteriores não é compatível com o modo FIPS e impedirá que ele seja instalado com sucesso. Você pode verificar se o modo FIPS está ativado usando o `fips-mode-setup --check` comando. Você pode desativar o modo FIPS usando o `fips-modesetup --disable` comando. Reinicie após desativar o modo FIPS para instalar com êxito o ONTAP Mediator 1,8 ou anterior.

- Você deve atualizar o Mediador ONTAP para a versão mais recente disponível. As versões anteriores do ONTAP Mediator permanecem retrocompatíveis com todas as versões do ONTAP, mas as versões recentes incluem patches de segurança para todos os elementos de terceiros.
- Quando você atualiza para uma nova versão do ONTAP Mediator, o instalador atualiza automaticamente para a versão SCST recomendada, a menos que uma versão superior esteja disponível. Para obter instruções sobre como instalar manualmente uma versão SCST mais alta, "Gerencie o serviço Mediator"consulte . Para versões suportadas, consulte "Matriz de suporte SCST".

> Se ocorrer uma falha de instalação, talvez seja necessário atualizar para uma versão posterior do ONTAP Mediator.

- Se você instalar o `yum-utils` pacote, você pode usar o `needs-restarting` comando.

Requisitos da OS

Seu sistema operacional deve atender aos seguintes requisitos:

- instalação física de 64 bits ou máquina virtual
- 8 GB DE RAM
- 1 GB de espaço em disco (usado para instalação de aplicativos, logs de servidor e banco de dados)
- Usuário: Acesso root

A tabela a seguir mostra os sistemas operacionais suportados para cada versão do ONTAP Mediator.

ONTAP versão mediadora	Versões Linux suportadas
1,9	• Red Hat Enterprise Linux ◦ Compatível: 8,4, 8,5, 8,6, 8,7, 8,9, 9,1 e 9,3 1 ◦ Recomendado: 8,8, 8,10, 9,0, 9,2, 9,4 e 9,5 • Rocky Linux 8 e 9
1,8	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 8,10, 9,0, 9,1, 9,2, 9,3 e 9,4 • Rocky Linux 8 e 9
1,7	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Rocky Linux 8 e 9
1,6	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2 • Rocky Linux 8 e 9
1,5	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,4	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3, 8,4, 8,5 • CentOS: 7,6, 7,7, 7,8, 7,9
1,3	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1, 8,2, 8,3 • CentOS: 7,6, 7,7, 7,8, 7,9
1,2	• Red Hat Enterprise Linux: 7,6, 7,7, 7,8, 7,9, 8,0, 8,1 • CentOS: 7,6, 7,7, 7,8, 7,9

1. Compatível significa que o RHEL não suporta mais esta versão, mas o ONTAP Mediator ainda pode ser instalado.

Considerações de atualização DO SO e compatibilidade do kernel

- Todos os pacotes de biblioteca, exceto o kernel, podem ser atualizados com segurança, mas podem exigir uma reinicialização para aplicar as alterações no aplicativo do Mediador ONTAP. Uma janela de serviço é recomendada quando uma reinicialização é necessária.
- Você deve manter o kernel do sistema operacional atualizado. O núcleo do kernel pode ser atualizado para uma versão listada como suportada no "Matriz de versão do Mediador ONTAP". Uma reinicialização é obrigatória, então você deve Planejar uma janela de manutenção para a interrupção.
  - Você deve desinstalar o módulo do kernel SCST antes de reiniciar e depois reinstalá-lo depois.
  - Você deve ter uma versão suportada do SCST pronta para reinstalar antes de iniciar a atualização do sistema operacional do kernel.

- A versão do kernel deve corresponder à versão do sistema operacional.
- A atualização para um kernel além da versão de SO suportada para a versão específica do Mediador ONTAP não é suportada. (Isso provavelmente indica que o módulo SCST testado não irá compilar).

Registre uma chave de segurança quando o UEFI Secure Boot estiver ativado

Para instalar o Mediador ONTAP com inicialização segura UEFI ativada, você deve Registrar uma chave de segurança antes que o serviço possa ser iniciado. A chave é gerada durante a etapa de compilação da instalação do SCST e salva como um par de chaves público-privado em sua máquina. Use o `mokutil` utilitário para adicionar a chave pública como uma chave de proprietário de máquina (MOK) ao firmware UEFI, permitindo que o sistema confie e carregue o módulo assinado. Salve a `mokutil` senha em um local seguro, pois isso é necessário ao reiniciar seu sistema para ativar o MOK.

Para determinar se o sistema está habilitado para UEFI e o Secure Boot está ativado, execute as seguintes etapas:

Passos

1. Se `mokutil` não estiver instalado, execute o seguinte comando:

   ```
   yum install mokutil
   ```

2. Verifique se o UEFI Secure Boot está ativado no seu sistema:

   ```
   mokutil --sb-state
   ```

   Os resultados indicam se o UEFI Secure Boot está ativado neste sistema.

   - Você é solicitado a criar uma senha que você deve armazenar em um local seguro. Você precisará dessa senha para ativar a chave no Gerenciador de Inicialização UEFI.
   - O ONTAP Mediator 1.2.0 e versões anteriores não suportam este modo.

3. Adicione a chave pública à lista MOK:

   ```
   mokutil --import
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
   r
   ```

   Você pode deixar a chave privada em seu local padrão ou movê-la para um local seguro. No entanto, a chave pública deve ser mantida em seu local existente para uso pelo Gerenciador de Inicialização. Para obter mais informações, consulte o seguinte arquivo de assinatura README.module:

   ```
   [root@hostname ~]# ls
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
   README.module-signing scst_module_key.der scst_module_key.priv
   ```

4. Reinicie o host e use o Gerenciador de Inicialização UEFI do dispositivo para aprovar o novo MOK. Você precisará da senha fornecida para o `mokutil` passo 2.

Desative o arranque seguro UEFI

Você também pode optar por desativar a Inicialização segura UEFI antes de instalar o ONTAP Mediator.

Passos

1. Nas configurações do BIOS da máquina física, desative a opção "UEFI Secure Boot".
2. Nas configurações da VMware para a VM, desative a opção "Início seguro" para o vSphere 6.x ou a opção "Inicialização segura" para o vSphere 7.x.

Atualize o sistema operacional host e, em seguida, o Mediador ONTAP

Para atualizar o sistema operacional do host para o ONTAP Mediator para uma versão posterior, você deve primeiro desinstalar o ONTAP Mediator.

Antes de começar

As melhores práticas para instalar o Red Hat Enterprise Linux ou Rocky Linux e os repositórios associados em seu sistema estão listados abaixo. Os sistemas instalados ou configurados de forma diferente podem exigir etapas adicionais.

- Você deve instalar o Red Hat Enterprise Linux ou Rocky Linux de acordo com as melhores práticas da Red Hat. Devido ao suporte de fim de vida para versões CentOS 8.x, não são recomendadas versões compatíveis do CentOS 8.x.
- Durante a instalação do serviço ONTAP Mediator no Red Hat Enterprise Linux ou Rocky Linux, o sistema deve ter acesso ao repositório apropriado para que o programa de instalação possa acessar e instalar todas as dependências de software necessárias.
- Para que o instalador do yum encontre software dependente nos repositórios Red Hat Enterprise Linux, você deve ter registrado o sistema durante a instalação do Red Hat Enterprise Linux ou depois usando uma assinatura válida do Red Hat.

  Consulte a documentação da Red Hat para obter informações sobre o Red Hat Subscription Manager.

- As seguintes portas devem ser não utilizadas e disponíveis para o Mediador:
  - 31784
  - 3260
- Se estiver a utilizar uma firewall de terceiros: Consulte "Requisitos de firewall para o ONTAP Mediator"
- Se o host Linux estiver em um local sem acesso à internet, você deve garantir que os pacotes necessários estejam disponíveis em um repositório local.

  Se você estiver usando o Link Aggregation Control Protocol (LACP) em um ambiente Linux, você deve configurar corretamente o kernel e certificar-se de que o `sysctl net.ipv4.conf.all.arp_ignore` está definido como "2".

O que você vai precisar

Os seguintes pacotes são exigidos pelo serviço Mediador ONTAP:

Todas as versões RHEL/CentOS	Pacotes adicionais para RHEL 8.x / Rocky Linux 8	Pacotes adicionais para RHEL 9.x / Rocky Linux 9

• openssl • openssl-devel • kernel-devel (uname -r) • gcc • marca • libselinux-utils • patch • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeMaker • efibootmgr • mokutil	• python3 pip • elfutils-libelf-devel • policycoreutils-python-utils • redhat-lsb-core • python39 • python39-nível	• python3 pip • elfutils-libelf-devel • policycoreutils-python-utils • python3 • python3-nível

O pacote de instalação Mediator é um arquivo tar compactado auto-extraível que inclui:

- Um arquivo RPM contendo todas as dependências que não podem ser obtidas do repositório da versão suportada.
- Um script de instalação.

Recomenda-se uma certificação SSL válida.

Sobre esta tarefa

Quando você atualiza o sistema operacional do host para o ONTAP Mediator para uma versão maior posterior (por exemplo, de 7.x para 8.x) usando a ferramenta leapp-upgrade, você deve desinstalar o ONTAP Mediator porque a ferramenta tenta detetar novas versões de quaisquer RPMs instalados nos repositórios que estão registrados no sistema.

Como um arquivo .rpm foi instalado como parte do instalador do ONTAP Mediator, ele está incluído nessa pesquisa. No entanto, como o arquivo .rpm foi descompactado como parte do instalador e não baixado de um repositório registrado, não é possível encontrar uma atualização. Neste caso, a ferramenta leapp-upgrade desinstala o pacote.

Para preservar os arquivos de log, que serão usados para triagem de casos de suporte, você deve fazer backup dos arquivos antes de fazer uma atualização do sistema operacional e restaurá-los após uma reinstalação do pacote do ONTAP Mediator. Como o Mediador ONTAP está sendo reinstalado, todos os clusters ONTAP que estão conetados a ele precisarão ser reconetados após a nova instalação.

As etapas a seguir devem ser executadas em ordem. Imediatamente após reinstalar o ONTAP Mediator, você deve parar o serviço ONTAP_Mediator, substituir os arquivos de log e reiniciar o serviço. Isso garantirá que os logs não sejam perdidos.

Passos

1. Faça uma cópia de segurança dos ficheiros de registo.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Execute a atualização com a ferramenta leapp-upgrade.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Reinstale o Mediador ONTAP.

> Execute o resto das etapas imediatamente após reinstalar o ONTAP Mediator para evitar a perda de arquivos de log.

```
[rootmediator-host ~]# ontap-mediator-1.9.0/ontap-mediator-1.9.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Pare o serviço ONTAP_Mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Substitua os arquivos de log.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Inicie o serviço ONTAP_Mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Reconecte todos os clusters do ONTAP ao mediador do ONTAP atualizado

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

Procedimento para sincronização ativa do SnapMirror

Para a sincronização ativa do SnapMirror, se você instalou o certificado TLS fora do diretório /opt/NetApp, então você não precisará reinstalá-lo. Se você estava usando o certificado autoassinado gerado padrão ou colocou seu certificado personalizado no diretório /opt/NetApp, então você deve fazer o backup e restaurá-lo.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA                         server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
```

```
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

Ativar o acesso aos repositórios

Você deve habilitar o acesso aos repositórios para que o ONTAP Mediator possa acessar os pacotes necessários durante o processo de instalação

Passos

1. Determine quais repositórios devem ser acessados, como mostrado na tabela a seguir:

Se o seu sistema operativo for…	Você deve fornecer acesso a esses repositórios…
RHEL 7.x	• rhel-7-server-optional-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
CentOS 7.x	• C7,6.1810 - repositório base
Rocky Linux 8	• appstream • base
Rocky Linux 9	• appstream • base

2. Use um dos procedimentos a seguir para habilitar o acesso aos repositórios listados acima para que o ONTAP Mediator possa acessar os pacotes necessários durante o processo de instalação.

Se o Mediador ONTAP tiver dependências nos módulos Python presentes nos repositórios "extras" e "opcionais", talvez seja necessário acessar os `rhel-X-for-x86_64-extras-rpms` arquivos e. `rhel-X-for-x86_64-optional-rpms`

Procedimento para o sistema operacional RHEL 7.x.

Use este procedimento se seu sistema operacional for **RHEL 7.x** para habilitar o acesso aos repositórios:

Passos

1. Assine o repositório necessário:

   ```
   subscription-manager repos --enable rhel-7-server-optional-rpms
   ```

   O exemplo a seguir mostra a execução deste comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-7-
   server-optional-rpms
   Repository 'rhel-7-server-optional-rpms' is enabled for this system.
   ```

2. Executar o `yum repolist` comando.

   O exemplo a seguir mostra a execução desse comando. O repositório "rhel-7-server-optional-rpms" deve aparecer na lista.

   ```
   [root@localhost ~]# yum repolist
   Loaded plugins: product-id, search-disabled-repos, subscription-
   manager
   rhel-7-server-optional-rpms | 3.2 kB  00:00:00
   rhel-7-server-rpms | 3.5 kB  00:00:00
   (1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
   |  26 kB  00:00:00
   (2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
   | 2.5 MB  00:00:00
   (3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
   | 8.3 MB  00:00:01
   repo id                                    repo name
   status
   rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
   Linux 7 Server - Optional (RPMs)   19,447
   rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
   Linux 7 Server (RPMs)              26,758
   repolist: 46,205
   [root@localhost ~]#
   ```

Procedimento para o sistema operacional RHEL 8.x.

Use este procedimento se seu sistema operacional for **RHEL 8.x** para habilitar o acesso aos repositórios:

Passos

1. Assine o repositório necessário:

   ```
   subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms

   subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
   ```

   O exemplo a seguir mostra a execução deste comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-baseos-rpms
   Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-appstream-rpms
   Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Executar o `yum repolist` comando.

   Os repositórios recém-inscritos devem aparecer na lista.

Procedimento para o sistema operacional RHEL 9.x.

Use este procedimento se seu sistema operacional for **RHEL 9.x** para habilitar o acesso aos repositórios:

Passos

1. Assine o repositório necessário:

   ```
   subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms

   subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
   ```

   O exemplo a seguir mostra a execução deste comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-baseos-rpms
   Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-appstream-rpms
   Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Executar o `yum repolist` comando.

   Os repositórios recém-inscritos devem aparecer na lista.

Procedimento para o sistema operacional CentOS 7.x.

Use este procedimento se o sistema operacional for **CentOS 7.x** para habilitar o acesso aos repositórios:

> Os exemplos a seguir mostram um repositório para o CentOS 7,6 e podem não funcionar para outras versões do CentOS. Use o repositório base para sua versão do CentOS.

Passos

1. Adicione o repositório C7,6.1810 - base. O repositório do C7,6.1810 - base Vault contém o pacote "kernel-devel" necessário para o ONTAP Mediator.
2. Adicione as seguintes linhas ao /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Executar o `yum repolist` comando.

   O exemplo a seguir mostra a execução desse comando. O repositório CentOS-7.6.1810 - base deve aparecer na lista.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Procedimento para sistemas operacionais Rocky Linux 8 ou 9

Use este procedimento se seu sistema operacional for **Rocky Linux 8** ou **Rocky Linux 9** para habilitar o acesso aos repositórios:

Passos

1. Assine os repositórios necessários:

   ```
   dnf config-manager --set-enabled baseos

   dnf config-manager --set-enabled appstream
   ```

2. Execute uma `clean` operação:

   ```
   dnf clean all
   ```

3. Verifique a lista de repositórios:

   ```
   dnf repolist
   ```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

Baixe o pacote de instalação do Mediator

Faça o download do pacote de instalação do Mediator como parte do processo de instalação.

Passos

1. Faça o download do pacote de instalação do Mediador na página do Mediador do ONTAP.

"Página de download do ONTAP Mediator"

2. Confirme se o pacote de instalação do Mediator está no diretório de trabalho atual:

```
[root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.9.0.tgz
```

```
ontap-mediator-1.9.0.tgz
```

> Para o ONTAP Mediator versões 1,4 e anteriores, o instalador é `ontap-mediator` chamado .

Se você estiver em um local sem acesso à internet, você deve garantir que o instalador tenha acesso aos pacotes necessários.

3. Se necessário, mova o pacote de instalação do Mediator do diretório de download para o diretório de instalação no host do Linux Mediator.
4. Descompacte o pacote de instalação:

`tar xvfz ontap-mediator-1.9.0.tgz`

```
ontap-mediator-1.9.0/
ontap-mediator-1.9.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/ONTAP-Mediator-production.pub
ontap-mediator-1.9.0/ontap-mediator-1.9.0
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig
```

Verifique a assinatura do código do ONTAP Mediator

Você deve verificar a assinatura do código do ONTAP Mediator antes de instalar o pacote de instalação do ONTAP Mediator.

Antes de começar

Antes de verificar a assinatura do código do ONTAP Mediator, o sistema deve atender aos seguintes requisitos.

- openssl versões 1.0.2 a 3,0 para verificação básica
- openssl versão 1.1.0 ou posterior para operações de Time Stamping Authority (TSA)
- Acesso público à Internet para verificação OCSP

Os seguintes arquivos estão incluídos no pacote de download:

Ficheiro	Descrição
`ONTAP-Mediator-production.pub`	A chave pública usada para verificar a assinatura
`csc-prod-chain-ONTAP-Mediator.pem`	A cadeia de confiança da CA de certificação pública
`csc-prod-ONTAP-Mediator.pem`	O certificado usado para gerar a chave
`ontap-mediator-1.9.0`	O executável de instalação do produto para a versão 1.9.0
`ontap-mediator-1.9.0.sig`	O hash SHA-256 e depois o RSA-assinado usando a chave csc-prod, assinatura para o instalador
`ontap-mediator-1.9.0.sig.tsr`	A solicitação de revogação para uso pelo OCSCP para a assinatura do instalador
`ontap-mediator-1.9.0.tsr`	O arquivo de solicitação de assinatura de carimbo de data/hora
`tsa-prod-ONTAP-Mediator.pem`	O certificado público para o TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	O certificado público CA Chain para o TSR

Passos

1. Efetue a verificação de revogação `csc-prod-ONTAP-Mediator.pem` utilizando o OCSP (Online Certificate Status Protocol).
   a. Localize o URL OCSP usado para Registrar o certificado porque os certificados de desenvolvedor podem não fornecer um uri.

      ```
      openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
      ```

   b. Gerar uma solicitação OCSP para o certificado.

      ```
      openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
      prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
      -reqout req.der
      ```

   c. Conete-se ao Gerenciador OCSP para enviar a solicitação OCSP:

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
chain-ONTAP-Mediator.pem
```

2. Verifique a cadeia de confiança do CSC e as datas de expiração em relação ao host local:

   `openssl verify`

   A `openssl` versão DO CAMINHO deve ter um válido `cert.pem` (não autoassinado).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Verifique os `ontap-mediator-1.9.0.sig.tsr` arquivos e `ontap-mediator-1.9.0.tsr` usando os certificados associados:

   `openssl ts -verify`

   `.tsr` os ficheiros contêm a resposta de carimbo de hora associada ao instalador e à assinatura de código. O processamento confirma que o carimbo de data/hora tem uma assinatura válida da TSA e que o seu ficheiro de entrada não foi alterado. A verificação é efetuada localmente na sua máquina. Independentemente, não há necessidade de acessar servidores TSA.

```
openssl ts -verify -data ontap-mediator-1.9.0.sig -in ontap-mediator-
1.9.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.9.0 -in ontap-mediator-
1.9.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
ONTAP-Mediator.pem
```

4. Verifique assinaturas contra a chave:

   `openssl -dgst -verify`

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.9.0.sig ontap-mediator-1.9.0
```

Exemplo de verificação da assinatura do código do ONTAP Mediator (saída do console)

```
[root@scspa2695423001 ontap-mediator-1.9.0]# pwd
/root/ontap-mediator-1.9.0
[root@scspa2695423001 ontap-mediator-1.9.0]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.9.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.9.0.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.9.0.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.9.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.9.0]#
[root@scspa2695423001 ontap-mediator-1.9.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.9.0.sig -in ontap-mediator-
1.9.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.9.0 -in ontap-mediator-
1.9.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.9.0.sig ontap-mediator-1.9.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.9.0]#
```

Instale o pacote de instalação do Mediador ONTAP

Para instalar o serviço Mediador ONTAP, você deve obter o pacote de instalação e executar o instalador no host.

Passos

1. Execute o instalador e responda aos prompts conforme necessário:

   `./ontap-mediator-1.9.0/ontap-mediator-1.9.0 -y`

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.9.0/ontap-mediator-1.9.0 -y
   ```

   O processo de instalação prossegue para criar as contas necessárias e instalar os pacotes necessários. Se você tiver uma versão anterior do Mediator instalada no host, você será solicitado a confirmar que deseja atualizar.

2. A partir do ONTAP Mediator 1,4, o mecanismo de Inicialização segura é ativado em sistemas UEFI. Quando o Secure Boot estiver ativado, você deve seguir etapas adicionais para Registrar a chave de segurança após a instalação:

   - Siga as instruções no arquivo README para assinar o módulo do kernel SCST.:

     `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

- Localize as teclas necessárias:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> Após a instalação, os arquivos README e a localização da chave também são fornecidos na saída do sistema.

Exemplo de instalação do Mediador ONTAP (saída do console)

```
[root@mediator_host ~]# cat /etc/os-release
NAME="Red Hat Enterprise Linux"
VERSION="9.4 (Plow)"
ID="rhel"
ID_LIKE="fedora"
VERSION_ID="9.4"
PLATFORM_ID="platform:el9"
PRETTY_NAME="Red Hat Enterprise Linux 9.4 (Plow)"
ANSI_COLOR="0;31"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:redhat:enterprise_linux:9::baseos"
HOME_URL="https://www.redhat.com/"
DOCUMENTATION_URL="https://access.redhat.com/documentation/en-
us/red_hat_enterprise_linux/9"
BUG_REPORT_URL="https://bugzilla.redhat.com/"

REDHAT_BUGZILLA_PRODUCT="Red Hat Enterprise Linux 9"
REDHAT_BUGZILLA_PRODUCT_VERSION=9.4
REDHAT_SUPPORT_PRODUCT="Red Hat Enterprise Linux"
REDHAT_SUPPORT_PRODUCT_VERSION="9.4"
[root@mediator_host ~]#

[root@mediator_host ~]# tar -zxvf ontap-mediator-1.9.0.tgz
ontap-mediator-1.9.0/
ontap-mediator-1.9.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.9.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.9.0/ONTAP-Mediator-production.pub
ontap-mediator-1.9.0/ontap-mediator-1.9.0
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.tsr
ontap-mediator-1.9.0/ontap-mediator-1.9.0.sig
[root@mediator_host ~]# ontap-mediator-1.9.0/ontap-mediator-1.9.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
```

```
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? y(es)/N(o): yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin



Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode


+ Checking for default Linux firewall


################################################################
Preparing for installation of ONTAP Mediator packages.


+ Installing required packages.


Last metadata expiration check: 0:15:55 ago on Thu 17 Oct 2024 09:06:29
AM EDT.
Package openssl-1:3.0.7-27.el9.x86_64 is already installed.
Package openssl-devel-1:3.0.7-27.el9.x86_64 is already installed.
Package kernel-devel-5.14.0-427.22.1.el9_4.x86_64 is already installed.
Package gcc-11.4.1-3.el9.x86_64 is already installed.
Package make-1:4.3-8.el9.x86_64 is already installed.
Package libselinux-utils-3.6-1.el9.x86_64 is already installed.
Package perl-Data-Dumper-2.174-462.el9.x86_64 is already installed.
Package bzip2-1.0.8-8.el9.x86_64 is already installed.
Package elfutils-libelf-devel-0.190-2.el9.x86_64 is already installed.
Package policycoreutils-python-utils-3.6-2.1.el9.noarch is already
```

```
installed.
Package python3-3.9.18-3.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
===========
 Package
Architecture                              Version
Repository                                                                  Size
================================================================================
================================================================================
================================================================================
===========
Installing:
 efibootmgr                                                                 x86_64
16-12.el9                                       rhel-9-for-x86_64-
baseos-rpms                                      48 k
 mokutil                                                                    x86_64
2:0.6.0-4.el9                                   rhel-9-for-x86_64-
baseos-rpms                                      50 k
 patch                                                                      x86_64
2.7.6-16.el9                                    rhel-9-for-x86_64-
appstream-rpms                                  130 k
 perl-ExtUtils-MakeMaker                                                    noarch
2:7.60-3.el9                                    rhel-9-for-x86_64-
appstream-rpms                                  304 k
 python3-devel                                                              x86_64
3.9.18-3.el9_4.5                                rhel-9-for-x86_64-
appstream-rpms                                  248 k
 python3-pip                                                                noarch
21.2.3-8.el9                                    rhel-9-for-x86_64-
appstream-rpms                                  2.0 M
Upgrading:
 openssl                                                                    x86_64
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
baseos-rpms                                     1.2 M
 openssl-devel                                                              x86_64
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
appstream-rpms                                  4.1 M
 openssl-libs                                                               i686
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
baseos-rpms                                     1.9 M
 openssl-libs                                                               x86_64
1:3.0.7-28.el9_4                                rhel-9-for-x86_64-
baseos-rpms                                     1.9 M
```

```
 python-unversioned-command                                    noarch
3.9.18-3.el9_4.5                                    rhel-9-for-x86_64-
appstream-rpms                                       10 k
 python3                                                       x86_64
3.9.18-3.el9_4.5                                    rhel-9-for-x86_64-
baseos-rpms                                          30 k
 python3-libs                                                  x86_64
3.9.18-3.el9_4.5                                    rhel-9-for-x86_64-
baseos-rpms                                         7.9 M
Installing dependencies:
 efi-filesystem                                                noarch
6-2.el9_0                                           rhel-9-for-x86_64-
baseos-rpms                                         9.5 k
 efivar-libs                                                   x86_64
38-3.el9                                            rhel-9-for-x86_64-
baseos-rpms                                         124 k
 perl-AutoSplit                                                noarch
5.74-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       22 k
 perl-Benchmark                                                noarch
1.23-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       27 k
 perl-CPAN-Meta-YAML                                           noarch
0.018-461.el9                                       rhel-9-for-x86_64-
appstream-rpms                                       29 k
 perl-Devel-PPPort                                             x86_64
3.62-4.el9                                          rhel-9-for-x86_64-
appstream-rpms                                      216 k
 perl-ExtUtils-Command                                         noarch
2:7.60-3.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       16 k
 perl-ExtUtils-Constant                                        noarch
0.25-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       49 k
 perl-ExtUtils-Install                                         noarch
2.20-4.el9                                          rhel-9-for-x86_64-
appstream-rpms                                       47 k
 perl-ExtUtils-Manifest                                        noarch
1:1.73-4.el9                                        rhel-9-for-x86_64-
appstream-rpms                                       37 k
 perl-ExtUtils-ParseXS                                         noarch
1:3.40-460.el9                                      rhel-9-for-x86_64-
appstream-rpms                                      190 k
 perl-File-Compare                                             noarch
1.100.600-481.el9                                   rhel-9-for-x86_64-
appstream-rpms                                       14 k
```

```
 perl-JSON-PP                                                  noarch
1:4.06-4.el9                                          rhel-9-for-x86_64-
appstream-rpms                                 69 k
 perl-Test-Harness                                             noarch
1:3.42-461.el9                                        rhel-9-for-x86_64-
appstream-rpms                                299 k
 perl-lib                                                      x86_64
0.65-481.el9                                          rhel-9-for-x86_64-
appstream-rpms                                 15 k
 perl-version                                                  x86_64
7:0.99.28-4.el9                                       rhel-9-for-x86_64-
appstream-rpms                                 67 k
 systemtap-sdt-devel                                           x86_64
5.0-4.el9                                             rhel-9-for-x86_64-
appstream-rpms                                 77 k
Installing weak dependencies:
 perl-CPAN-Meta                                                noarch
2.150010-460.el9                                      rhel-9-for-x86_64-
appstream-rpms                                206 k
 perl-CPAN-Meta-Requirements                                   noarch
2.140-461.el9                                         rhel-9-for-x86_64-
appstream-rpms                                 34 k
 perl-devel                                                    x86_64
4:5.32.1-481.el9                                      rhel-9-for-x86_64-
appstream-rpms                                680 k
 perl-doc                                                      noarch
5.32.1-481.el9                                        rhel-9-for-x86_64-
appstream-rpms                                4.6 M

Transaction Summary
================================================================================
================================================================================
================================================================================
===========
Install  27 Packages
Upgrade   7 Packages

Total download size: 27 M
Is this ok [y/N]: y
Downloading Packages:
(1/34): perl-CPAN-Meta-YAML-0.018-461.el9.noarch.rpm
220 kB/s |  29 kB     00:00
(2/34): perl-CPAN-Meta-Requirements-2.140-461.el9.noarch.rpm
249 kB/s |  34 kB     00:00
(3/34): perl-ExtUtils-Install-2.20-4.el9.noarch.rpm
4.2 MB/s |  47 kB     00:00
```

```
(4/34): perl-CPAN-Meta-2.150010-460.el9.noarch.rpm
1.3 MB/s | 206 kB     00:00
(5/34): perl-version-0.99.28-4.el9.x86_64.rpm
5.5 MB/s |  67 kB     00:00
(6/34): perl-ExtUtils-Manifest-1.73-4.el9.noarch.rpm
3.9 MB/s |  37 kB     00:00
(7/34): perl-ExtUtils-MakeMaker-7.60-3.el9.noarch.rpm
16 MB/s | 304 kB     00:00
(8/34): perl-ExtUtils-ParseXS-3.40-460.el9.noarch.rpm
11 MB/s | 190 kB     00:00
(9/34): patch-2.7.6-16.el9.x86_64.rpm
15 MB/s | 130 kB     00:00
(10/34): perl-Test-Harness-3.42-461.el9.noarch.rpm
15 MB/s | 299 kB     00:00
(11/34): perl-Devel-PPPort-3.62-4.el9.x86_64.rpm
14 MB/s | 216 kB     00:00
(12/34): perl-ExtUtils-Command-7.60-3.el9.noarch.rpm
1.4 MB/s |  16 kB     00:00
(13/34): perl-JSON-PP-4.06-4.el9.noarch.rpm
6.9 MB/s |  69 kB     00:00
(14/34): perl-Benchmark-1.23-481.el9.noarch.rpm
3.9 MB/s |  27 kB     00:00
(15/34): systemtap-sdt-devel-5.0-4.el9.x86_64.rpm
9.4 MB/s |  77 kB     00:00
(16/34): perl-AutoSplit-5.74-481.el9.noarch.rpm
2.8 MB/s |  22 kB     00:00
(17/34): perl-ExtUtils-Constant-0.25-481.el9.noarch.rpm
5.9 MB/s |  49 kB     00:00
(18/34): perl-File-Compare-1.100.600-481.el9.noarch.rpm
1.7 MB/s |  14 kB     00:00
(19/34): perl-devel-5.32.1-481.el9.x86_64.rpm
21 MB/s | 680 kB     00:00
(20/34): perl-lib-0.65-481.el9.x86_64.rpm
2.1 MB/s |  15 kB     00:00
(21/34): python3-pip-21.2.3-8.el9.noarch.rpm
26 MB/s | 2.0 MB     00:00
(22/34): efi-filesystem-6-2.el9_0.noarch.rpm
1.8 MB/s | 9.5 kB     00:00
(23/34): python3-devel-3.9.18-3.el9_4.5.x86_64.rpm
8.6 MB/s | 248 kB     00:00
(24/34): efibootmgr-16-12.el9.x86_64.rpm
5.0 MB/s |  48 kB     00:00
(25/34): efivar-libs-38-3.el9.x86_64.rpm
15 MB/s | 124 kB     00:00
(26/34): mokutil-0.6.0-4.el9.x86_64.rpm
5.2 MB/s |  50 kB     00:00
```

```
(27/34): python-unversioned-command-3.9.18-3.el9_4.5.noarch.rpm
2.2 MB/s |  10 kB     00:00
(28/34): python3-3.9.18-3.el9_4.5.x86_64.rpm
6.9 MB/s |  30 kB     00:00
(29/34): perl-doc-5.32.1-481.el9.noarch.rpm
27 MB/s | 4.6 MB     00:00
(30/34): openssl-3.0.7-28.el9_4.x86_64.rpm
30 MB/s | 1.2 MB     00:00
(31/34): openssl-devel-3.0.7-28.el9_4.x86_64.rpm
25 MB/s | 4.1 MB     00:00
(32/34): openssl-libs-3.0.7-28.el9_4.x86_64.rpm
22 MB/s | 1.9 MB     00:00
(33/34): openssl-libs-3.0.7-28.el9_4.i686.rpm
29 MB/s | 1.9 MB     00:00
(34/34): python3-libs-3.9.18-3.el9_4.5.x86_64.rpm
27 MB/s | 7.9 MB     00:00
--------------------------------------------------------------------------
--------------------------------------------------------------------------
--------------------------------------------------------------------------
-----------
Total
44 MB/s |  27 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Upgrading        : openssl-libs-1:3.0.7-28.el9_4.x86_64
1/41
  Installing       : perl-version-7:0.99.28-4.el9.x86_64
2/41
  Installing       : perl-CPAN-Meta-Requirements-2.140-461.el9.noarch
3/41
  Upgrading        : python3-libs-3.9.18-3.el9_4.5.x86_64
4/41
  Upgrading        : python3-3.9.18-3.el9_4.5.x86_64
5/41
  Upgrading        : python-unversioned-command-3.9.18-3.el9_4.5.noarch
6/41
  Installing       : efivar-libs-38-3.el9.x86_64
7/41
  Installing       : perl-File-Compare-1.100.600-481.el9.noarch
8/41
  Installing       : perl-JSON-PP-1:4.06-4.el9.noarch
```

```
9/41
  Installing       : perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch
10/41
  Installing       : python3-pip-21.2.3-8.el9.noarch
11/41
  Installing       : systemtap-sdt-devel-5.0-4.el9.x86_64
12/41
  Installing       : efi-filesystem-6-2.el9_0.noarch
13/41
  Installing       : perl-lib-0.65-481.el9.x86_64
14/41
  Installing       : perl-doc-5.32.1-481.el9.noarch
15/41
  Installing       : perl-ExtUtils-Constant-0.25-481.el9.noarch
16/41
  Installing       : perl-AutoSplit-5.74-481.el9.noarch
17/41
  Installing       : perl-Benchmark-1.23-481.el9.noarch
18/41
  Installing       : perl-Test-Harness-1:3.42-461.el9.noarch
19/41
  Installing       : perl-ExtUtils-Command-2:7.60-3.el9.noarch
20/41
  Installing       : perl-Devel-PPPort-3.62-4.el9.x86_64
21/41
  Installing       : perl-ExtUtils-Manifest-1:1.73-4.el9.noarch
22/41
  Installing       : perl-CPAN-Meta-YAML-0.018-461.el9.noarch
23/41
  Installing       : perl-CPAN-Meta-2.150010-460.el9.noarch
24/41
  Installing       : perl-devel-4:5.32.1-481.el9.x86_64
25/41
  Installing       : perl-ExtUtils-Install-2.20-4.el9.noarch
26/41
  Installing       : perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch
27/41
  Installing       : efibootmgr-16-12.el9.x86_64
28/41
  Installing       : python3-devel-3.9.18-3.el9_4.5.x86_64
29/41
  Installing       : mokutil-2:0.6.0-4.el9.x86_64
30/41
  Upgrading        : openssl-devel-1:3.0.7-28.el9_4.x86_64
31/41
  Upgrading        : openssl-1:3.0.7-28.el9_4.x86_64
```

```
32/41
  Installing       : patch-2.7.6-16.el9.x86_64
33/41
  Upgrading        : openssl-libs-1:3.0.7-28.el9_4.i686
34/41
  Cleanup          : openssl-devel-1:3.0.7-27.el9.x86_64
35/41
  Cleanup          : python-unversioned-command-3.9.18-3.el9.noarch
36/41
  Cleanup          : openssl-1:3.0.7-27.el9.x86_64
37/41
  Cleanup          : openssl-libs-1:3.0.7-27.el9.i686
38/41
  Cleanup          : python3-3.9.18-3.el9.x86_64
39/41
  Cleanup          : python3-libs-3.9.18-3.el9.x86_64
40/41
  Cleanup          : openssl-libs-1:3.0.7-27.el9.x86_64
41/41
  Running scriptlet: openssl-libs-1:3.0.7-27.el9.x86_64
41/41
  Verifying        : perl-CPAN-Meta-2.150010-460.el9.noarch
1/41
  Verifying        : perl-CPAN-Meta-Requirements-2.140-461.el9.noarch
2/41
  Verifying        : perl-CPAN-Meta-YAML-0.018-461.el9.noarch
3/41
  Verifying        : perl-ExtUtils-Install-2.20-4.el9.noarch
4/41
  Verifying        : perl-version-7:0.99.28-4.el9.x86_64
5/41
  Verifying        : perl-ExtUtils-MakeMaker-2:7.60-3.el9.noarch
6/41
  Verifying        : perl-ExtUtils-Manifest-1:1.73-4.el9.noarch
7/41
  Verifying        : perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch
8/41
  Verifying        : perl-Test-Harness-1:3.42-461.el9.noarch
9/41
  Verifying        : patch-2.7.6-16.el9.x86_64
10/41
  Verifying        : perl-Devel-PPPort-3.62-4.el9.x86_64
11/41
  Verifying        : perl-ExtUtils-Command-2:7.60-3.el9.noarch
12/41
  Verifying        : perl-JSON-PP-1:4.06-4.el9.noarch
```

```
13/41
  Verifying        : perl-Benchmark-1.23-481.el9.noarch
14/41
  Verifying        : python3-pip-21.2.3-8.el9.noarch
15/41
  Verifying        : systemtap-sdt-devel-5.0-4.el9.x86_64
16/41
  Verifying        : perl-AutoSplit-5.74-481.el9.noarch
17/41
  Verifying        : perl-ExtUtils-Constant-0.25-481.el9.noarch
18/41
  Verifying        : perl-File-Compare-1.100.600-481.el9.noarch
19/41
  Verifying        : perl-devel-4:5.32.1-481.el9.x86_64
20/41
  Verifying        : perl-doc-5.32.1-481.el9.noarch
21/41
  Verifying        : perl-lib-0.65-481.el9.x86_64
22/41
  Verifying        : python3-devel-3.9.18-3.el9_4.5.x86_64
23/41
  Verifying        : efi-filesystem-6-2.el9_0.noarch
24/41
  Verifying        : efibootmgr-16-12.el9.x86_64
25/41
  Verifying        : efivar-libs-38-3.el9.x86_64
26/41
  Verifying        : mokutil-2:0.6.0-4.el9.x86_64
27/41
  Verifying        : python-unversioned-command-3.9.18-3.el9_4.5.noarch
28/41
  Verifying        : python-unversioned-command-3.9.18-3.el9.noarch
29/41
  Verifying        : openssl-devel-1:3.0.7-28.el9_4.x86_64
30/41
  Verifying        : openssl-devel-1:3.0.7-27.el9.x86_64
31/41
  Verifying        : python3-3.9.18-3.el9_4.5.x86_64
32/41
  Verifying        : python3-3.9.18-3.el9.x86_64
33/41
  Verifying        : python3-libs-3.9.18-3.el9_4.5.x86_64
34/41
  Verifying        : python3-libs-3.9.18-3.el9.x86_64
35/41
  Verifying        : openssl-1:3.0.7-28.el9_4.x86_64
```

```
36/41
  Verifying        : openssl-1:3.0.7-27.el9.x86_64
37/41
  Verifying        : openssl-libs-1:3.0.7-28.el9_4.x86_64
38/41
  Verifying        : openssl-libs-1:3.0.7-27.el9.x86_64
39/41
  Verifying        : openssl-libs-1:3.0.7-28.el9_4.i686
40/41
  Verifying        : openssl-libs-1:3.0.7-27.el9.i686
41/41
Installed products updated.

Upgraded:
  openssl-1:3.0.7-28.el9_4.x86_64       openssl-devel-1:3.0.7-
28.el9_4.x86_64       openssl-libs-1:3.0.7-28.el9_4.i686       openssl-
libs-1:3.0.7-28.el9_4.x86_64       python-unversioned-command-3.9.18-
3.el9_4.5.noarch
  python3-3.9.18-3.el9_4.5.x86_64       python3-libs-3.9.18-
3.el9_4.5.x86_64
Installed:
  efi-filesystem-6-2.el9_0.noarch
efibootmgr-16-12.el9.x86_64                          efivar-libs-38-
3.el9.x86_64                          mokutil-2:0.6.0-4.el9.x86_64
  patch-2.7.6-16.el9.x86_64                                  perl-
AutoSplit-5.74-481.el9.noarch                  perl-Benchmark-1.23-
481.el9.noarch                  perl-CPAN-Meta-2.150010-
460.el9.noarch
  perl-CPAN-Meta-Requirements-2.140-461.el9.noarch           perl-
CPAN-Meta-YAML-0.018-461.el9.noarch             perl-Devel-PPPort-
3.62-4.el9.x86_64                perl-ExtUtils-Command-2:7.60-
3.el9.noarch
  perl-ExtUtils-Constant-0.25-481.el9.noarch                 perl-
ExtUtils-Install-2.20-4.el9.noarch             perl-ExtUtils-
MakeMaker-2:7.60-3.el9.noarch          perl-ExtUtils-Manifest-1:1.73-
4.el9.noarch
  perl-ExtUtils-ParseXS-1:3.40-460.el9.noarch                perl-
File-Compare-1.100.600-481.el9.noarch          perl-JSON-PP-1:4.06-
4.el9.noarch                  perl-Test-Harness-1:3.42-
461.el9.noarch
  perl-devel-4:5.32.1-481.el9.x86_64                         perl-doc-
5.32.1-481.el9.noarch                      perl-lib-0.65-
481.el9.x86_64                          perl-version-7:0.99.28-
4.el9.x86_64
  python3-devel-3.9.18-3.el9_4.5.x86_64                      python3-
pip-21.2.3-8.el9.noarch                    systemtap-sdt-devel-5.0-
```

```
4.el9.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.T7uce6/ontap-
mediator-1.9.0/ontap-mediator-1.9.0/install_20241017092214.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20241017092214.log)

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README

[root@mediator_host ~]# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Thu 2024-10-17 09:27:14 EDT; 1min
12s ago
    Process: 54470
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 54489 (uwsgi)
     Status: "uWSGI is ready"
      Tasks: 3 (limit: 11104)
     Memory: 77.1M
        CPU: 2.507s
     CGroup: /system.slice/ontap_mediator.service
             ├─54489 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
```

```
             ├─54504 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
             └─54507 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Creating
filesystem with 192000 4k blocks and 48000 inodes
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Filesystem UUID:
b1fa0a40-0e7d-4c67-bbff-33421f3ec61b
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Superblock backups
stored on blocks:
Oct 17 09:27:10 mediator_host ontap_mediator[54476]:         32768,
98304, 163840
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: [41B blob data]
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: [38B blob data]
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: Creating journal
(4096 blocks): done
Oct 17 09:27:10 mediator_host ontap_mediator[54476]: [75B blob data]
Oct 17 09:27:10 mediator_host ontap_mediator[54489]: [uWSGI] getting
INI configuration from
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
Oct 17 09:27:14 mediator_host systemd[1]: Started ONTAP Mediator.

[root@mediator_host ~]# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Thu 2024-10-17 09:27:08 EDT; 1min
32s ago
    Process: 54384 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 54467 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 54425 (iscsi-scstd)
      Tasks: 1 (limit: 11104)
     Memory: 1.2M
        CPU: 494ms
     CGroup: /system.slice/mediator-scst.service
             └─54425 /usr/local/sbin/iscsi-scstd

Oct 17 09:27:07 mediator_host systemd[1]: Starting mediator-
scst.service...
Oct 17 09:27:08 mediator_host iscsi-scstd[54423]: max_data_seg_len
1048576, max_queued_cmds 2048
Oct 17 09:27:08 mediator_host scst[54384]: Loading and configuring SCST
Oct 17 09:27:08 mediator_host systemd[1]: Started mediator-
```

```
scst.service.
[root@mediator_host ~]#
```

Verifique a instalação

Após a instalação do Mediador ONTAP, você deve verificar se os serviços do Mediador ONTAP estão em execução.

Passos

1. Veja o status dos serviços do Mediador ONTAP:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme as portas usadas pelo serviço do Mediador ONTAP:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

Configuração pós-instalação

Depois que o serviço do Mediador ONTAP for instalado e executado, tarefas de configuração adicionais devem ser executadas no sistema de storage ONTAP para usar os recursos do Mediador:

- Para usar o serviço Mediador ONTAP em uma configuração IP do MetroCluster, "Configurando o serviço do Mediador ONTAP a partir de uma configuração IP do MetroCluster"consulte .
- Para usar a sincronização ativa do SnapMirror, "Instale o Serviço do Mediador ONTAP e confirme a configuração do cluster do ONTAP"consulte .

Configurar as políticas de segurança do ONTAP Mediator

O servidor Mediador ONTAP suporta várias configurações de segurança configuráveis. Os valores padrão para todas as configurações são fornecidos em um `low_space_threshold_mib: 10` arquivo somente leitura:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Todos os valores colocados no `ontap_mediator.user_config.yaml` substituirão os valores padrão e serão mantidos em todas as atualizações do ONTAP Mediator.

Depois de modificar `ontap_mediator.user_config.yaml`, reinicie o serviço ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Modifique os atributos do Mediador ONTAP

Os atributos do Mediador ONTAP descritos nesta seção podem ser modificados se necessário.

> Outros valores padrão no `ontap_mediator.config.yaml` não devem ser alterados porque os valores modificados não são mantidos durante as atualizações do ONTAP Mediator.

Você modifica os atributos do Mediador do ONTAP copiando as variáveis necessárias `ontap_mediator.user_config.yaml` para o arquivo para substituir as configurações padrão.

Instale certificados SSL de terceiros

Se você precisar substituir os certificados autoassinados padrão por certificados SSL de terceiros, modifique determinados atributos nos seguintes arquivos:

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

As variáveis nesses arquivos são usadas para controlar os arquivos de certificado usados pelo serviço do Mediador ONTAP.

As variáveis padrão listadas na tabela a seguir são incluídas no `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` arquivo.

Variável	Caminho
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` é usado para definir a expiração dos certificados de cliente. O valor máximo é de três anos (1095 dias).
- `x509_passin_pwd` é a senha para o certificado de cliente assinado.

As variáveis padrão listadas na tabela a seguir são incluídas no `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` arquivo.

Variável	Caminho
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt`

Se você modificar esses atributos, reinicie o serviço do ONTAP Mediator para aplicar as alterações. Para obter instruções detalhadas sobre como substituir certificados padrão por certificados de terceiros, "Substitua certificados autoassinados por certificados de terceiros confiáveis"consulte .

Proteção contra ataque por senha

As configurações a seguir fornecem proteção contra ataques de adivinhação de senha de força bruta.

Para ativar a funcionalidade, defina um valor para a `window_seconds` e a `retry_limit`.

Exemplos:

- Forneça uma janela de 5 minutos para suposições e, em seguida, redefina a contagem para zero falhas:

  ```
  authentication_lock_window_seconds: 300
  ```

- Bloqueie a conta se ocorrerem cinco falhas dentro do período de tempo da janela:

  ```
  authentication_retry_limit: 5
  ```

- Reduza o impactos de ataques de adivinhação de senha de força bruta definindo um atraso que ocorre antes de rejeitar cada tentativa, o que retarda os ataques.

  ```
  authentication_failure_delay_seconds: 5
  ```

  ```
  authentication_failure_delay_seconds: 0   # seconds (float) to delay
  failed auth attempts prior to response, 0 = no delay
  authentication_lock_window_seconds: null  # seconds (int) since the
  oldest failure before resetting the retry counter, null = no window
  authentication_retry_limit: null          # number of retries to allow
  before locking API access, null = unlimited
  ```

Regras de complexidade de senha

Os campos a seguir controlam as regras de complexidade de senha da conta de usuário da API do ONTAP Mediator.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

Controle do espaço livre

Existem definições que controlam o espaço livre necessário no `/opt/netapp/lib/ontap_mediator` disco.

Se o espaço for inferior ao limite definido, o serviço emitirá um evento de aviso.

```
low_space_threshold_mib: 10
```

Controle do espaço de Registro de reserva

O RESERVE_LOG_SPACE é controlado por configurações específicas. Por padrão, a instalação do servidor Mediador do ONTAP cria um espaço em disco separado para os logs. O instalador cria um novo arquivo de tamanho fixo com um total de 700 MB de espaço em disco para ser usado explicitamente para o Registro do Mediator.

Para desativar esse recurso e usar o espaço em disco padrão, execute as seguintes etapas:

1. Altere o valor de RESERVE_LOG_SPACE de 1 para 0 no seguinte arquivo:

   `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

2. Reinicie o Mediator:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

Para reativar a funcionalidade, altere o valor de 0 para 1 e reinicie o Mediador.

> Alternar entre espaços de disco não limpa logs existentes. Todos os logs anteriores são copiados e movidos para o espaço em disco atual depois de alternar e reiniciar o Mediator.

Gerenciar o serviço de mediador do ONTAP

Gerencie o serviço do ONTAP Mediator, incluindo alteração das credenciais do usuário, interrupção e reativação do serviço, verificação de sua integridade e instalação ou desinstalação do SCST para manutenção do host. Você também pode gerenciar certificados, como a geração de certificados autoassinados, a substituição deles por certificados de terceiros confiáveis e a solução de problemas relacionados a certificados.

Altere o nome de usuário

Você pode alterar o nome de usuário usando o procedimento a seguir.

Sobre esta tarefa

Execute esta tarefa no host Linux no qual o serviço Mediador ONTAP está instalado.

Se você não conseguir alcançar esse comando, talvez seja necessário executar o comando usando o caminho completo como mostrado no exemplo a seguir:

```
/usr/local/bin/mediator_username
```

Passos

Altere o nome de usuário escolhendo uma das seguintes opções:

- **Opção (a)**: Execute o comando `mediator_change_user` e responda aos prompts como mostrado no exemplo a seguir:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- **Opção (b)**: Execute o seguinte comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

Altere a palavra-passe

Pode alterar a palavra-passe utilizando o seguinte procedimento.

Sobre esta tarefa

Execute esta tarefa no host Linux no qual o serviço Mediador ONTAP está instalado.

Se você não conseguir alcançar esse comando, talvez seja necessário executar o comando usando o caminho completo como mostrado no exemplo a seguir:

```
/usr/local/bin/mediator_change_password
```

Passos

Altere a senha escolhendo uma das seguintes opções:

- **Opção (a)**: Execute o `mediator_change_password` comando e responda aos prompts como mostrado no exemplo a seguir:

```
 [root@mediator-host ~]# mediator_change_password
 Change the Mediator API password by entering the following values:
    Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
          Confirm Password:
 The password has been updated successfully.
 [root@mediator-host ~]#
```

- **Opção (b)**: Execute o seguinte comando:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

O exemplo mostra que a senha foi alterada de "mediator1" para "mediator2".

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

Pare o serviço Mediador ONTAP

Para interromper o serviço do Mediador ONTAP, execute as seguintes etapas:

Passos

1. Pare o Mediador ONTAP:

   ```
   systemctl stop ontap_mediator
   ```

2. Parar SCST:

   ```
   systemctl stop mediator-scst
   ```

3. Desative o Mediador ONTAP e o SCST:

   ```
   systemctl diable ontap_mediator mediator-scst
   ```

Reative o serviço Mediador ONTAP

Para reativar o serviço do Mediador ONTAP, execute as seguintes etapas:

Passos

1. Ative o Mediador ONTAP e o SCST:

   ```
   systemctl enable ontap_mediator mediator-scst
   ```

2. Iniciar SCST:

   ```
   systemctl start mediator-scst
   ```

3. Iniciar o Mediador ONTAP:

   ```
   systemctl start ontap_mediator
   ```

Verifique se o Mediador ONTAP está saudável

Após a instalação do Mediador ONTAP, você deve verificar se os serviços do Mediador ONTAP estão em execução.

Passos

1. Veja o status dos serviços do Mediador ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme as portas usadas pelo serviço do Mediador ONTAP:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Desinstale manualmente o SCST para executar a manutenção do host

Para desinstalar o SCST, você precisa do pacote tar SCST que é usado para a versão instalada do ONTAP Mediator.

Passos

1. Baixe o pacote SCST apropriado (como mostrado na tabela a seguir) e descompacte-o.

Para esta versão …	Use este pacote tar…
ONTAP Mediador 1,9	scst-3,8.0.tar.bz2
ONTAP Mediador 1,8	scst-3,8.0.tar.bz2
ONTAP Mediador 1,7	scst-3,7.0.tar.bz2
ONTAP Mediador 1,6	scst-3,7.0.tar.bz2
ONTAP Mediador 1,5	scst-3,6.0.tar.bz2
ONTAP Mediador 1,4	scst-3,6.0.tar.bz2
ONTAP Mediador 1,3	scst-3,5.0.tar.bz2
ONTAP Mediador 1,1	scst-3,4.0.tar.bz2
ONTAP Mediador 1,0	scst-3,3.0.tar.bz2

2. Emita os seguintes comandos no diretório "scst":
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Instale manualmente o SCST para executar a manutenção do host

Para instalar manualmente o SCST, você precisa do pacote tar SCST que é usado para a versão instalada do ONTAP Mediator (consulte a tabela acima).

1. Emita os seguintes comandos no diretório "scst":
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`
   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`
2. Opcionalmente, se o Secure Boot estiver ativado, antes de reiniciar, execute as seguintes etapas:
   a. Determine cada nome de arquivo para os módulos "scst_vdisk", "scst" e "iscsi_scst":

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

   b. Determine a versão do kernel:

```
[root@localhost ~]# uname -r
```

   c. Assine cada arquivo com o kernel:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der \
_module-filename_
```

   d. Instale a chave correta com o firmware UEFI.

      As instruções para instalar a chave UEFI estão localizadas em:

      `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

A chave UEFI gerada está localizada em:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der
```

3. Execute uma reinicialização:

```
reboot
```

Desinstale o serviço ONTAP Mediator

Se necessário, pode remover o serviço Mediador ONTAP.

Antes de começar

O Mediador ONTAP tem de ser desligado do ONTAP antes de remover o serviço Mediador ONTAP.

Sobre esta tarefa

Você precisa executar esta tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.

Se você não conseguir alcançar esse comando, talvez seja necessário executar o comando usando o caminho completo como mostrado no exemplo a seguir:

```
/usr/local/bin/uninstall_ontap_mediator
```

Passo

1. Desinstale o serviço ONTAP Mediator:

```
uninstall_ontap_mediator
```

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Regenerar um certificado temporário autoassinado

A partir do ONTAP Mediator 1,7, você pode regenerar um certificado auto-assinado temporário usando o seguinte procedimento.

> Este procedimento só é suportado em sistemas que executam o ONTAP Mediator 1,7 ou posterior.

Sobre esta tarefa

- Você executa essa tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.

- Só é possível executar esta tarefa se os certificados autoassinados gerados se tornarem obsoletos devido a alterações no nome de host ou endereço IP do host após a instalação do Mediador ONTAP.
- Depois que o certificado auto-assinado temporário for substituído por um certificado de terceiros confiável, você *não* usará essa tarefa para regenerar um certificado. A ausência de um certificado auto-assinado fará com que este procedimento falhe.

Passo

Para regenerar um novo certificado auto-assinado temporário para o host atual, execute o seguinte passo:

1. Reinicie o serviço do Mediador ONTAP:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

   ```
   [root@xyz000123456 ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
   [root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

   Adding Subject Alternative Names to the self-signed server certificate
   #
   # OpenSSL example configuration file.
   Generating self-signed certificates
   Generating RSA private key, 4096 bit long modulus (2 primes)
   ..........................................................................
   ..........................................................................
   ..................++++
   ..........................................................++++
   e is 65537 (0x010001)
   Generating a RSA private key
   ..............................................++++
   ..........................................................................
   ..........................................................................+++
   +
   writing new private key to 'ontap_mediator_server.key'
   -----
   Signature ok
   subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
   ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
   support@netapp.com
   Getting CA Private Key
   ```

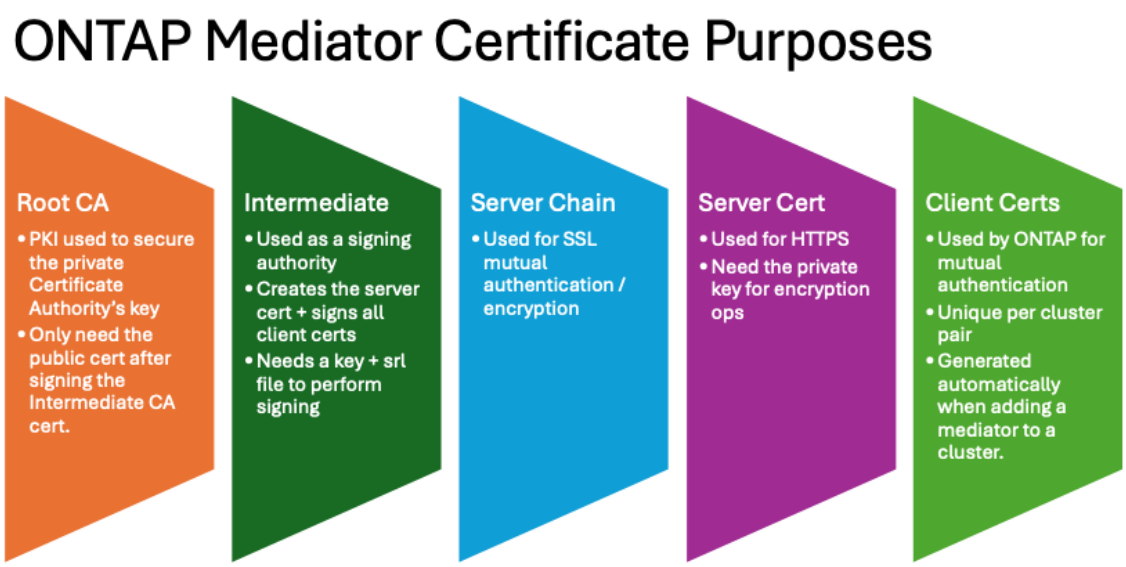
Substitua certificados autoassinados por certificados de terceiros confiáveis

Se suportado, você pode substituir certificados autoassinados por certificados de terceiros confiáveis.

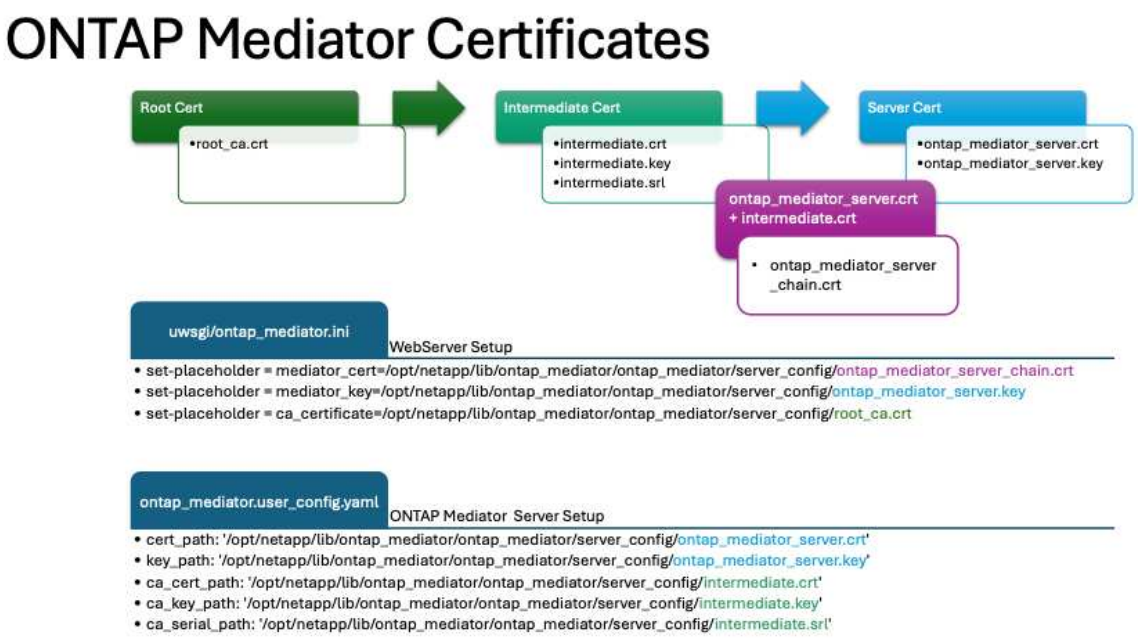
- Os certificados de terceiros são suportados apenas a partir do ONTAP 9.16,1 e em algumas versões de patch anteriores do ONTAP. "NetApp Bugs Online ID de erro CONTAP-243278"Consulte .
- Os certificados de terceiros são suportados apenas em sistemas que executam o ONTAP Mediator 1,7 ou posterior.

Sobre esta tarefa

- Você executa essa tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.
- Você pode executar esta tarefa se os certificados autoassinados gerados precisarem ser substituídos por certificados obtidos de uma autoridade de certificação subordinada (CA) confiável. Para isso, você deve ter acesso a uma autoridade de infraestrutura de chave pública (PKI) confiável.
- A imagem a seguir mostra as finalidades de cada certificado do Mediador ONTAP.



- A imagem a seguir mostra a configuração para a configuração do servidor web e a configuração do servidor do ONTAP Mediator.



Etapa 1: Obter um certificado de um terceiro que emite um certificado de CA

Você pode obter um certificado de uma autoridade PKI usando o procedimento a seguir.

O exemplo a seguir demonstra a substituição dos agentes de certificados autoassinados, ou seja, `ca.key` `ca.csr` `ca.srl` , e `ca.crt` localizados em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` por agentes de certificados de terceiros.

> O exemplo ilustra os critérios necessários para os certificados necessários para o serviço Mediador ONTAP. Você pode obter os certificados de uma autoridade PKI de uma forma que pode ser diferente deste procedimento. Ajuste o procedimento de acordo com a necessidade do seu negócio.

Passos

1. Crie uma chave `ca.key` privada e um arquivo de configuração `openssl_ca.cnf` que serão consumidos pela autoridade PKI para gerar um certificado.

   a. Gerar a chave privada `ca.key` :

   Exemplo

```
openssl genrsa -aes256 -out ca.key 4096
```

   a. O arquivo de `openssl_ca.cnf` configuração (localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define as propriedades que o certificado gerado deve ter.

2. Use a chave privada e o arquivo de configuração para criar uma solicitação de assinatura de certificado `ca.csr` :

Exemplo:

```
openssl req -key <private_key_name>.key -new -out <certificate_csr_name>.csr
-config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new -config
openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIE6TCCAtECAQAwgaMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh
...
erARKhY9z0e8BHPl3g==
-----END CERTIFICATE REQUEST-----
```

3. Envie a solicitação de assinatura de certificado `ca.csr` para uma autoridade PKI para sua assinatura.

   A autoridade PKI verifica a solicitação e assina o `.csr`, gerando o certificado `ca.crt`. Além disso, você precisa obter o `root_ca.crt` certificado que assinou o `ca.crt` certificado da autoridade PKI.

> Para clusters do SnapMirror Business Continuity (SM-BC), é necessário adicionar os `ca.crt` certificados e `root_ca.crt` a um cluster do ONTAP. "Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

Etapa 2: Gere um certificado de servidor assinando com uma certificação de CA de terceiros

Um certificado de servidor deve ser assinado pela chave privada `ca.key` e pelo certificado de `ca.crt` terceiros . Além disso, o arquivo de configuração `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contém certos atributos que especificam as propriedades necessárias para certificados de servidor emitidos pelo OpenSSL.

Os comandos a seguir podem gerar um certificado de servidor.

Passos

1. Para gerar uma solicitação de assinatura de certificado de servidor (CSR), execute o seguinte comando `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` na pasta:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. para gerar um certificado de servidor a partir do CSR, execute o seguinte comando a partir `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` da pasta:

> Os `ca.crt` arquivos e `ca.key` foram obtidos de uma autoridade PKI. Se estiver a utilizar um nome de certificado diferente, por exemplo, `intermediate.crt` e `intermediate.key`, substitua `ca.crt` e `ca.key` por `intermediate.crt` e `intermediate.key` respetivamente.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt -CAkey
ca.key -CAcreateserial -sha512 -days 1095 -req -in ontap_mediator_server.csr
-out ontap_mediator_server.crt
```

- A `-CAcreateserial` opção é usada para gerar os `ca.srl` arquivos ou `intermediate.srl`, dependendo do nome do certificado que você está usando.

Etapa 3: Substitua o novo certificado de CA de terceiros e o certificado de servidor na configuração do ONTAP Mediator

A configuração do certificado é fornecida ao serviço do Mediador ONTAP no arquivo de configuração localizado em `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. O arquivo inclui os seguintes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediato
r_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` e `key_path` são variáveis de certificado de servidor.
- `ca_cert_path`, `ca_key_path`, E `ca_serial_path` são variáveis de certificado CA.

Passos

1. Substitua todos `ca.*` os arquivos por certificados de terceiros.
2. Crie uma cadeia de certificados a partir dos `ca.crt` certificados e `ontap_mediator_server.crt`:

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ficheiro.

   Atualizar os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_ser
   ver_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_ser
   ver.key
   ```

```
set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- `mediator_key value`O é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.

4. Verifique se os seguintes atributos dos certificados recém-gerados estão definidos corretamente:
   - Proprietário do Grupo Linux: `netapp:netapp`
   - Permissões do Linux: `600`
5. Reinicie o Mediador ONTAP:

```
systemctl restart ontap_mediator
```

Passo 4: Opcionalmente, use um caminho ou nome diferente para seus certificados de terceiros

Você pode usar certificados de terceiros com um nome diferente `ca.*` ou armazenar os certificados de terceiros em um local diferente.

Passos

1. Configure o `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` arquivo para substituir os valores de variável padrão no `ontap_mediator.config.yaml` arquivo.

   Se você tiver obtido `intermediate.crt` de uma autoridade PKI e armazenar sua chave privada `intermediate.key` no local `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, o `ontap_mediator.user_config.yaml` arquivo deverá ser parecido com o seguinte exemplo:

> Se você usou `intermediate.crt` para assinar o `ontap_mediator_server.crt` certificado, o `intermediate.srl` arquivo será gerado. Consulte Etapa 2: Gere um certificado de servidor assinando com uma certificação de CA de terceiros para obter mais informações.

```
[root@scs000216655 server_config]# cat  ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the following
key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediat
e.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediat
e.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediat
e.srl'
```

a. Se estiver a utilizar uma estrutura de certificados onde o `root_ca.crt` certificado forneça um `intermediate.crt` certificado que assine o `ontap_mediator_server.crt` certificado, crie uma cadeia de certificados a partir dos `intermediate.crt` certificados e `ontap_mediator_server.crt`:

> Você deve ter obtido os `intermediate.crt` certificados e `ontap_mediator_server.crt` de uma autoridade PKI anteriormente no procedimento.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Atualize o `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` ficheiro.

Atualizar os valores de `mediator_cert`, `mediator_key` e `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_s
erver_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_s
erver.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- O `mediator_cert` valor é o caminho do `ontap_mediator_server_chain.crt` arquivo.
- O `mediator_key` valor é o caminho da chave no `ontap_mediator_server.crt` arquivo, que é `ontap_mediator_server.key`.
- O `ca_certificate` valor é o caminho do `root_ca.crt` arquivo.

> Para clusters do SnapMirror Business Continuity (SM-BC), é necessário adicionar os `intermediate.crt` certificados e `root_ca.crt` a um cluster do ONTAP. "Configure o Mediador e os clusters do ONTAP para a sincronização ativa do SnapMirror"Consulte .

c. Verifique se os seguintes atributos dos certificados recém-gerados estão definidos corretamente:
   - Proprietário do Grupo Linux: `netapp:netapp`
   - Permissões do Linux: `600`

2. Reinicie o Mediador ONTAP quando os certificados forem atualizados no arquivo de configuração:

```
systemctl restart ontap_mediator
```

Solucionar problemas relacionados ao certificado

Você pode verificar certas propriedades dos certificados.

Verifique a expiração do certificado

Use o seguinte comando para identificar o intervalo de validade do certificado:

```
[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

Verifique as extensões X509v3 na certificação CA

Use o comando a seguir para verificar as extensões X509v3 na certificação CA.

As propriedades definidas em **`v3_ca`** em `openssl_ca.cnf` são apresentadas como `X509v3 extensions` em `ca.crt`.

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

Verifique as extensões X509v3 nos nomes Alt do certificado do servidor e do assunto

As `v3_req` propriedades definidas no `openssl_server.cnf` arquivo de configuração são exibidas como `X509v3 extensions` no certificado.

No exemplo a seguir, você pode obter as variáveis nas `alt_names` seções executando os comandos `hostname -A` e `hostname -I` na VM Linux na qual o Mediador ONTAP está instalado.

Verifique com o administrador da rede os valores corretos das variáveis.

```
[root@scs000216982 server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@scs000216982 server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@scs000216982 server_config]# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Verifique se uma chave privada corresponde a um certificado

Você pode verificar se uma chave particular corresponde a um certificado.

Use os seguintes comandos OpenSSL na chave e no certificado respetivamente:

```
[root@scs000216982 server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@scs000216982 server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Se o `-modulus` atributo para ambos corresponder, ele indica que a chave privada e o par de certificados são compatíveis e podem funcionar entre si.

Verifique se um certificado de servidor é criado a partir de um certificado de CA específico

Você pode usar o comando a seguir para verificar se o certificado do servidor foi criado a partir de um certificado de CA específico.

```
[root@scs000216982 server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Se a validação OCSP (Online Certificate Status Protocol) estiver sendo usada, use o comando "verificação do openssl".

Mantenha o host do SO para o ONTAP Mediator

Para um desempenho ideal, você deve manter o sistema operacional do host para o ONTAP Mediator regularmente.

Reinicie o host

Reinicie o host quando os clusters estiverem saudáveis. Embora o Mediador ONTAP esteja offline, os clusters correm o risco de não poderem reagir adequadamente às falhas. Recomenda-se uma janela de serviço se for necessário reiniciar.

O Mediador ONTAP será retomado automaticamente durante uma reinicialização e reentrará as relações que foram configuradas anteriormente com clusters ONTAP.

Atualizações do pacote de host

Qualquer biblioteca ou pacote yum (exceto o kernel) pode ser atualizado com segurança, mas pode exigir uma reinicialização para entrar em vigor. Recomenda-se uma janela de serviço se for necessário reiniciar.

Se você instalar o `yum-utils` pacote, use o `needs-restarting` comando para detetar se alguma alteração de pacote requer uma reinicialização.

Você deve reiniciar se alguma das dependências do ONTAP Mediator for atualizada porque elas não terão efeito imediato nos processos em execução.

Atualizações menores do kernel do sistema operacional do host

SCST deve ser compilado para o kernel que está sendo usado. Para atualizar o SO, é necessária uma janela de manutenção.

Passos

Execute as etapas a seguir para atualizar o kernel do sistema operacional do host.

1. Pare o Mediador ONTAP
2. Desinstale o pacote SCST. (O SCST não fornece um mecanismo de atualização.)
3. Atualize o sistema operacional e reinicie.
4. Volte a instalar o pacote SCST.
5. Reative os serviços do Mediador ONTAP.

O host muda para o nome de host ou IP

Sobre esta tarefa

- Você executa essa tarefa no host Linux no qual o serviço do Mediador ONTAP está instalado.
- Só é possível executar esta tarefa se os certificados autoassinados gerados se tornarem obsoletos devido a alterações no nome de host ou endereço IP do host após a instalação do Mediador ONTAP.
- Depois que o certificado auto-assinado temporário for substituído por um certificado de terceiros confiável, você *não* usará essa tarefa para regenerar um certificado. A ausência de um certificado auto-assinado fará com que este procedimento falhe.

Passo

Para regenerar um novo certificado auto-assinado temporário para o host atual, execute o seguinte passo:

1. Reinicie o Mediador ONTAP:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Gerenciamento de site IP do MetroCluster com o Gerenciador do sistema

As configurações do MetroCluster espelham os dados e a configuração de forma síncrona entre dois clusters ONTAP em locais separados. A partir do ONTAP 9.8, você pode usar o Gerenciador de sistema como uma interface simplificada para gerenciar uma configuração IP do MetroCluster.

> Você só pode executar operações do MetroCluster usando o Gerenciador de sistema em uma configuração IP do MetroCluster. Em uma configuração MetroCluster FC, você ainda pode usar o Gerenciador do sistema para gerenciar cada nó na configuração do MetroCluster, mas não pode executar nenhuma operação específica do MetroCluster.

Normalmente, você configura e configura clusters em uma configuração do MetroCluster em dois locais geográficos separados. Em seguida, configure o peering entre os clusters para que eles sincronizem e compartilhem dados. Os dois clusters na rede com peering fornecem recuperação de desastres (DR)

bidirecional, onde cada cluster pode ser a origem e o backup do outro cluster. Em configurações IP do MetroCluster de oito ou quatro nós, cada local consiste em controladores de storage configurados como um ou dois pares de alta disponibilidade (HA).

Em um terceiro local, é possível "Instale o serviço do Mediador ONTAP"monitorar o estado dos nós e seus parceiros de DR. O serviço de Mediador ONTAP pode implementar um switchover não planejado assistido por Mediador (MAUSO) em caso de desastre.

Você também pode executar um switchover negociado a fim de reduzir um dos clusters para manutenção planejada. O cluster de parceiros manipula todas as operações de e/S de dados dos dois clusters até você abrir o cluster no qual você realizou a manutenção e executar uma operação de switchback.

Você pode encontrar procedimentos para configurar e gerenciar uma configuração IP do MetroCluster usando o Gerenciador de sistema no "Documentação do MetroCluster".

Proteção de dados usando backup em fita

Visão geral do backup em fita do FlexVol volumes

O ONTAP oferece suporte a backup e restauração em fita por meio do protocolo NDMP (Network Data Management Protocol). O NDMP permite que você faça backup de dados em sistemas de armazenamento diretamente para fita, resultando em uso eficiente da largura de banda da rede. O ONTAP suporta ambos os motores dump e SMTape para backup em fita.

Você pode executar um backup ou restauração de despejo ou SMTape usando aplicativos de backup compatíveis com NDMP. Apenas a versão NDMP 4 é suportada.

Backup em fita usando despejo

Dump é um backup baseado em cópia Snapshot no qual os dados do sistema de arquivos são copiados para a fita. O mecanismo de despejo do ONTAP faz backup de arquivos, diretórios e as informações da lista de controle de acesso (ACL) aplicáveis à fita. É possível fazer backup de um volume inteiro, de uma qtree inteira ou de uma subárvore que não seja um volume inteiro ou uma qtree inteiro. O dump suporta backups de linha de base, diferenciais e incrementais.

Backup em fita usando SMTape

O SMTape é uma solução de recuperação de desastres baseada em cópia Snapshot da ONTAP que faz backup de blocos de dados em fita. Você pode usar o SMTape para realizar backups de volume em fitas. No entanto, você não pode executar um backup no nível de qtree ou subárvore. O SMTape suporta backups de linha de base, diferenciais e incrementais.

A partir do ONTAP 9.13,1, o backup de fita usando Sincronização ativa do SnapMirroro SMTape é compatível com o .

Fluxo de trabalho de backup e restauração em fita

Você pode executar operações de backup e restauração em fita usando um aplicativo de backup habilitado para NDMP.

Sobre esta tarefa

O fluxo de trabalho de backup e restauração de fita fornece uma visão geral das tarefas envolvidas na execução de operações de backup e restauração de fita. Para obter informações detalhadas sobre como executar uma operação de backup e restauração, consulte a documentação do aplicativo de backup.

Passos

1. Configure uma configuração de biblioteca de fitas escolhendo uma topologia de fita compatível com NDMP.
2. Habilite serviços NDMP em seu sistema de storage.

   Você pode ativar os serviços NDMP no nível de nó ou no nível de máquina virtual de storage (SVM). Isso depende do modo NDMP no qual você optar por executar a operação de backup e restauração de fita.

3. Use as opções NDMP para gerenciar o NDMP em seu sistema de storage.

   Você pode usar opções NDMP no nível de nó ou no nível SVM. Isso depende do modo NDMP no qual você optar por executar a operação de backup e restauração de fita.

   Você pode modificar as opções NDMP no nível do nó usando o `system services ndmp modify` comando e no nível SVM usando o `vserver services ndmp modify` comando. Para obter mais informações sobre esses comandos, consulte as páginas man.

4. Execute uma operação de backup ou restauração em fita usando um aplicativo de backup habilitado para NDMP.

   O ONTAP suporta ambos os motores dump e SMTape para backup e restauração de fita.

   Para obter mais informações sobre como usar o aplicativo de backup (também chamado de *Data Management Applications* ou *DMAs*) para executar operações de backup ou restauração, consulte a documentação do aplicativo de backup.

Informações relacionadas

Topologias comuns de backup de fita NDMP

Compreender o motor de descarga para volumes FlexVol

Casos de uso para escolher um mecanismo de backup de fita

O ONTAP suporta dois mecanismos de backup: SMTape e dump. Você deve estar ciente dos casos de uso dos mecanismos de backup SMTape e dump para ajudá-lo a escolher o mecanismo de backup para executar operações de backup e restauração de fita.

O despejo pode ser usado nos seguintes casos:

- Direct Access Recovery (DAR) de arquivos e diretórios
- Backup de um subconjunto de subdiretórios ou arquivos em um caminho específico
- Excluindo arquivos e diretórios específicos durante backups
- Preservando o backup por longos períodos

SMTape pode ser usado nos seguintes casos:

- Solução de recuperação de desastres

- Preservar a economia de deduplicação e as configurações de deduplicação nos dados de backup durante uma operação de restauração
- Backup de grandes volumes

Gerenciar unidades de fita

Visão geral de gerenciar unidades de fita

Você pode verificar as conexões da biblioteca de fitas e exibir informações da unidade de fita antes de executar uma operação de backup ou restauração de fita. Você pode usar uma unidade de fita não qualificada emulando-a em uma unidade de fita qualificada. Você também pode atribuir e remover aliases de fita, além de exibir aliases existentes.

Quando você faz backup de dados para fita, os dados são armazenados em arquivos de fita. As marcas de arquivo separam os arquivos de fita e os arquivos não têm nomes. Você especifica um arquivo de fita pela sua posição na fita. Você escreve um arquivo de fita usando um dispositivo de fita. Ao ler o arquivo de fita, você deve especificar um dispositivo que tenha o mesmo tipo de compactação usado para gravar esse arquivo de fita.

Comandos para gerenciar unidades de fita, trocadores de Mídia e operações de unidade de fita

Existem comandos para visualizar informações sobre unidades de fita e trocadores de Mídia em um cluster, colocar uma unidade de fita on-line e colocá-la off-line, modificar a posição do cartucho da unidade de fita, definir e limpar o nome do alias da unidade de fita e redefinir uma unidade de fita. Você também pode exibir e redefinir estatísticas de unidade de fita.

Se você quiser…	Use este comando…
Coloque uma unidade de fita on-line	`storage tape online`
Limpe um nome de alias para unidade de fita ou trocador de Mídia	`storage tape alias clear`
Ative ou desative uma operação de rastreamento de fita para uma unidade de fita	`storage tape trace`
Modifique a posição do cartucho da unidade de fita	`storage tape position`
Redefina uma unidade de fita	`storage tape reset` Este comando está disponível apenas no nível avançado de privilégios.
Defina um nome de alias para unidade de fita ou trocador de Mídia	`storage tape alias set`

Se você quiser…	Use este comando…
Tire uma unidade de fita off-line	`storage tape offline`
Veja informações sobre todas as unidades de fita e trocadores de Mídia	`storage tape show`
Exibir informações sobre unidades de fita conetadas ao cluster	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Veja informações sobre os modificadores de Mídia conetados ao cluster	`storage tape show-media-changer`
Exibir informações de erro sobre unidades de fita conetadas ao cluster	`storage tape show-errors`
Veja todas as unidades de fita qualificadas e compatíveis do ONTAP conetadas a cada nó no cluster	`storage tape show-supported-status`
Exibir aliases de todas as unidades de fita e alteradores de Mídia conetados a cada nó no cluster	`storage tape alias show`
Redefina a leitura de estatísticas de uma unidade de fita para zero	`storage stats tape zero tape_name` Você deve usar este comando no nodeshell.
Ver unidades de fita suportadas pelo ONTAP	`storage show tape supported [-v]` Você deve usar este comando no nodeshell. Você pode usar a `-v` opção para exibir mais detalhes sobre cada unidade de fita.
Veja as estatísticas do dispositivo de fita para entender o desempenho da fita e verificar o padrão de uso	`storage stats tape tape_name` Você deve usar este comando no nodeshell.

Para obter mais informações sobre esses comandos, consulte as páginas man.

Use uma unidade de fita não qualificada

Você pode usar uma unidade de fita não qualificada em um sistema de storage se ele puder emular uma unidade de fita qualificada. É então Tratado como uma unidade de fita qualificada. Para usar uma unidade de fita não qualificada, primeiro você deve determinar se ela emula qualquer uma das unidades de fita qualificadas.

Sobre esta tarefa

Uma unidade de fita não qualificada é aquela que está conetada ao sistema de storage, mas não é suportada

ou reconhecida pela ONTAP.

Passos

1. Visualize as unidades de fita não qualificadas conetadas a um sistema de armazenamento usando o `storage tape show-supported-status` comando.

   O comando a seguir exibe as unidades de fita conetadas ao sistema de armazenamento e o status de suporte e qualificação de cada unidade de fita. As unidades de fita não qualificadas também são listadas. `tape_drive_vendor_name` É uma unidade de fita não qualificada conetada ao sistema de storage, mas não suportada pelo ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Emular a unidade de fita qualificada.

   "Downloads do NetApp: Arquivos de configuração do dispositivo de fita"

Informações relacionadas

Quais são as unidades de fita qualificadas

Atribua aliases de fita

Para facilitar a identificação do dispositivo, você pode atribuir aliases de fita a uma unidade de fita ou trocador de médio porte. Os aliases fornecem uma correspondência entre os nomes lógicos dos dispositivos de backup e um nome atribuído permanentemente à unidade de fita ou ao trocador de Mídia.

Passos

1. Atribua um alias a uma unidade de fita ou trocador de médio usando o `storage tape alias set` comando.

   Para obter mais informações sobre esse comando, consulte as páginas man.

   Você pode visualizar as informações do número de série (SN) sobre as unidades de fita usando o `system`

`node hardware tape drive show` comando e sobre bibliotecas de fitas usando os `system node hardware tape library show` comandos.

O comando a seguir define um nome de alias para uma unidade de fita com o número de série SN[123456]L4 anexado ao nó, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

O comando a seguir define um nome de alias para um trocador de Mídia com número de série SN[65432] anexado ao nó, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

Informações relacionadas

O que é a distorção da fita

Removendo aliases de fita

Remover aliases de fita

Você pode remover aliases usando o `storage tape alias clear` comando quando aliases persistentes não são mais necessários para uma unidade de fita ou um trocador de médio.

Passos

1. Remova um alias de uma unidade de fita ou trocador de médio usando o `storage tape alias clear` comando.

   Para obter mais informações sobre esse comando, consulte as páginas man.

   O comando a seguir remove os aliases de todas as unidades de fita especificando o escopo da operação de eliminação de alias para `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Depois de terminar

Se você estiver executando uma operação de backup ou restauração de fita usando NDMP, depois de remover um alias de uma unidade de fita ou trocador de médio porte, você deve atribuir um novo nome de alias à unidade de fita ou trocador de médio para continuar o acesso ao dispositivo de fita.

Informações relacionadas

O que é a distorção da fita

Atribuindo aliases de fita

Ativar ou desativar reservas de fita

Você pode controlar como o ONTAP gerencia as reservas de dispositivos de fita usando a `tape.reservations` opção. Por padrão, a reserva de fita é desativada.

Sobre esta tarefa

Ativar a opção de reservas de fita pode causar problemas se as unidades de fita, trocadores médios, pontes ou bibliotecas não funcionarem corretamente. Se os comandos de fita relatarem que o dispositivo está reservado quando nenhum outro sistema de armazenamento está usando o dispositivo, essa opção deve ser desativada.

Passos

1. Para usar o mecanismo de reserva/Liberação SCSI ou SCSI Persistent Reservationsor para desativar as reservas de fita, digite o seguinte comando no clustershell:

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi` Seleciona o mecanismo de reserva/Liberação SCSI.

   `persistent` Seleciona as reservas persistentes SCSI.

   `off` desativa as reservas de fita.

Informações relacionadas

Quais são as reservas de fita

Comandos para verificar as conexões da biblioteca de fitas

Você pode exibir informações sobre o caminho de conexão entre um sistema de armazenamento e uma configuração de biblioteca de fitas conetada ao sistema de armazenamento. Você pode usar essas informações para verificar o caminho de conexão para a configuração da biblioteca de fitas ou para solucionar problemas relacionados aos caminhos de conexão.

Você pode exibir os detalhes da biblioteca de fitas a seguir para verificar as conexões da biblioteca de fitas depois de adicionar ou criar uma nova biblioteca de fitas, ou depois de restaurar um caminho com falha em um acesso de caminho único ou multipath a uma biblioteca de fitas. Você também pode usar essas informações ao solucionar erros relacionados ao caminho ou se o acesso a uma biblioteca de fitas falhar.

- Nó ao qual a biblioteca de fitas está conetada
- ID do dispositivo
- Caminho NDMP
- Nome da biblioteca de fitas
- IDs da porta de destino e da porta do iniciador
- Acesso de caminho único ou multipath a uma biblioteca de fitas para cada porta de destino ou iniciador de FC
- Detalhes de integridade de dados relacionados ao caminho, como "'erros de caminho'" e "'caminho qual'"
- Grupos LUN e contagens LUN

Se você quiser…	Use este comando…
Exibir informações sobre uma biblioteca de fitas em um cluster	`system node hardware tape library show`
Exibir informações de caminho para uma biblioteca de fitas	`storage tape library path show`
Exibir informações de caminho para uma biblioteca de fitas para cada porta do iniciador	`storage tape library path show-by-initiator`
Exibir informações de conetividade entre uma biblioteca de fitas de armazenamento e um cluster	`storage tape library config show`

Para obter mais informações sobre esses comandos, consulte as páginas man.

Sobre unidades de fita

Visão geral das unidades de fita qualificadas

Você deve usar uma unidade de fita qualificada que tenha sido testada e encontrada para funcionar corretamente em um sistema de armazenamento. Você pode seguir a distorção da fita e também ativar as reservas de fita para garantir que apenas um sistema de armazenamento acesse uma unidade de fita em qualquer momento específico.

Uma unidade de fita qualificada é uma unidade de fita que foi testada e encontrada para funcionar corretamente em sistemas de armazenamento. Você pode qualificar unidades de fita para versões existentes do ONTAP usando o arquivo de configuração de fita.

Formato do ficheiro de configuração da cassete

O formato do arquivo de configuração da fita consiste em campos como ID do fornecedor, ID do produto e detalhes dos tipos de compactação para uma unidade de fita. Este arquivo também consiste em campos opcionais para ativar o recurso de autoload de uma unidade de fita e alterar os valores de tempo limite do comando de uma unidade de fita.

A tabela a seguir exibe o formato do arquivo de configuração da fita:

Item	Tamanho	Descrição
`vendor_id` (string)	até 8 bytes	O ID do fornecedor conforme relatado pelo `SCSI Inquiry` comando.
`product_id`(string)	até 16 bytes	O ID do produto conforme relatado pelo `SCSI Inquiry` comando.

Item	Tamanho	Descrição
`id_match_size`(número)		O número de bytes do ID do produto a ser usado para correspondência para detetar a unidade de fita a ser identificada, começando com o primeiro caractere do ID do produto nos dados de consulta.
`vendor_pretty` (string)	até 16 bytes	Se este parâmetro estiver presente, ele será especificado pela cadeia de carateres exibida pelo comando `storage tape show -device-names`; caso contrário, INQ_VENDOR_ID será exibido.
`product_pretty`(string)	até 16 bytes	Se este parâmetro estiver presente, ele será especificado pela cadeia de carateres exibida pelo comando `storage tape show -device-names`; caso contrário, INQ_PRODUCT_ID será exibido.

Os `vendor_pretty` campos e `product_pretty` são opcionais, mas se um desses campos tiver um valor, o outro também deve ter um valor.

A tabela a seguir explica a descrição, o código de densidade e o algoritmo de compressão para os vários tipos de compactação, como `l`, `m`, `h` e `a`:

Item	Tamanho	Descrição
`{l	m	h
a}_description=(string)`	até 24 bytes	A cadeia de carateres a imprimir para o comando nodeshell , `sysconfig -t`, que descreve as caraterísticas da configuração de densidade específica.
`{l	m	h
a}_density=(hex codes)`		O código de densidade a ser definido no descritor de bloco de página do modo SCSI correspondente ao código de densidade desejado para l, m, h ou a.

Item	Tamanho	Descrição
`{l	m	h
a}_algorithm=(hex codes)`		O algoritmo de compressão a ser definido na página do modo de compressão SCSI correspondente ao código de densidade e à caraterística de densidade desejada.

A tabela a seguir descreve os campos opcionais disponíveis no arquivo de configuração da fita:

Campo	Descrição
`autoload=(Boolean yes/no)`	Este campo é definido como `yes` se a unidade de fita tiver um recurso de carregamento automático; ou seja, depois que o cartucho de fita é inserido, a unidade de fita fica pronta sem a necessidade de executar um `SCSI load` comando (unidade de inicialização/parada). A predefinição para este campo é `no`.
`cmd_timeout_0x`	Valor de tempo limite individual. Você deve usar este campo somente se quiser especificar um valor de tempo limite diferente daquele que está sendo usado como padrão pelo driver de fita. O arquivo de exemplo lista os valores padrão de tempo limite do comando SCSI usados pela unidade de fita. O valor de tempo limite pode ser expresso em minutos (m), segundos (s) ou milissegundos (ms). Não deve alterar este campo.

Você pode baixar e exibir o arquivo de configuração de fita no site de suporte da NetApp.

Exemplo de um formato de arquivo de configuração de fita

O formato de arquivo de configuração de fita para a unidade de fita HP LTO5 ULTRIUM é o seguinte:

`vendor_id`"HP"

`product_id`Ultrium 5-SCSI

`id_match_size`9

`vendor_pretty`Hewlett-Packard

`product_pretty`"LTO-5"

`l_description`LTO-3(ro)/4 4/800GB"

`l_density`0x00

`l_algorithm`0x00

`m_description`LTO-3(ro)/4 8/1600GB cmp"

`m_density`0x00

`m_algorithm`0 x 01

`h_description`"LTO-5 1600GB"

`h_density`0 x 58

`h_algorithm`0x00

`a_description`LTO-5 3200GB cmp

`a_density`0 x 58

`a_algorithm`0 x 01

`autoload`"sim"

Informações relacionadas

"Ferramentas do NetApp: Arquivos de configuração do dispositivo de fita"

Como o sistema de armazenamento qualifica uma nova unidade de fita dinamicamente

O sistema de armazenamento qualifica uma unidade de fita dinamicamente, combinando a ID do fornecedor e a ID do produto com as informações contidas na tabela de qualificação da fita.

Quando você coneta uma unidade de fita ao sistema de armazenamento, ela procura uma correspondência de ID de fornecedor e ID de produto entre as informações obtidas durante a descoberta de fita e as informações na tabela de qualificação de fita interna. Se o sistema de armazenamento detetar uma correspondência, ele marca a unidade de fita como qualificada e pode acessar a unidade de fita. Se o sistema de armazenamento não conseguir encontrar uma correspondência, a unidade de fita permanece no estado não qualificado e não é acessada.

Visão geral dos dispositivos de fita

Visão geral dos dispositivos de fita

Um dispositivo de fita é uma representação de uma unidade de fita. É uma combinação específica do tipo de rebobinagem e capacidade de compressão de uma unidade de fita.

Um dispositivo de fita é criado para cada combinação de tipo de rebobinagem e capacidade de compressão. Portanto, uma unidade de fita ou biblioteca de fitas pode ter vários dispositivos de fita associados a ela. Você deve especificar um dispositivo de fita para mover, gravar ou ler fitas.

Quando você instala uma unidade de fita ou uma biblioteca de fitas em um sistema de armazenamento, o ONTAP cria dispositivos de fita associados à unidade de fita ou à biblioteca de fitas.

O ONTAP deteta unidades de fita e bibliotecas de fitas e atribui números lógicos e dispositivos de fita a elas. O ONTAP deteta as bibliotecas e unidades de fita Fibre Channel, SAS e SCSI paralelo quando elas são conetadas às portas de interface. O ONTAP deteta essas unidades quando suas interfaces estão ativadas.

Formato do nome do dispositivo de fita

Cada dispositivo de fita tem um nome associado que aparece em um formato definido. O formato inclui informações sobre o tipo de dispositivo, tipo de rebobinagem, alias e tipo de compressão.

O formato do nome de um dispositivo de fita é o seguinte:

`rewind_type st alias_number compression_type`

`rewind_type` é o tipo de rebobinagem.

A lista a seguir descreve os vários valores do tipo de rebobinagem:

- **r**

  ONTAP rebobinam a fita depois que ela termina de escrever o arquivo de fita.

- **nº**

  O ONTAP não volta a gravar a fita depois de terminar de escrever o arquivo de fita. Você deve usar esse tipo de rebobinagem quando quiser gravar vários arquivos de fita na mesma fita.

- **ur**

  Este é o tipo de retorno de descarga/recarga. Quando você usa esse tipo de rebobinagem, a biblioteca de fitas descarrega a fita quando ela chega ao final de um arquivo de fita e, em seguida, carrega a próxima fita, se houver uma.

  Você deve usar esse tipo de rebobinagem somente nas seguintes circunstâncias:

  - A unidade de fita associada a esse dispositivo está em uma biblioteca de fitas ou está em um trocador médio que está no modo de biblioteca.
  - A unidade de fita associada a este dispositivo está conetada a um sistema de armazenamento.
  - Fitas suficientes para a operação que você está executando estão disponíveis na sequência de fitas da biblioteca definida para esta unidade de fita.

> Se você gravar uma fita usando um dispositivo sem rebobinagem, você deve rebobinar a fita antes de lê-la.

`st` é a designação padrão para uma unidade de fita.

`alias_number` É o alias que o ONTAP atribui à unidade de fita. Quando o ONTAP deteta uma nova unidade de fita, o ONTAP atribui um alias à unidade de fita.

`compression_type` é um código específico da unidade para a densidade de dados na fita e o tipo de compressão.

A lista a seguir descreve os vários valores para `compression_type`:

- **a**

  Compressão mais elevada

- **h**

  Alta compressão

- **m**

  Compressão média

- **l**

  Baixa compressão

Exemplos

`nrst0a` especifica um dispositivo sem rebobinagem na unidade de fita 0 usando a compressão mais alta.

Exemplo de uma lista de dispositivos de fita

O exemplo a seguir mostra os dispositivos de fita associados ao HP Ultrium 2-SCSI:

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
    rst0l  -  rewind device,        format is: HP (200GB)
    nrst0l -  no rewind device,     format is: HP (200GB)
    urst0l -  unload/reload device, format is: HP (200GB)
    rst0m  -  rewind device,        format is: HP (200GB)
    nrst0m -  no rewind device,     format is: HP (200GB)
    urst0m -  unload/reload device, format is: HP (200GB)
    rst0h  -  rewind device,        format is: HP (200GB)
    nrst0h -  no rewind device,     format is: HP (200GB)
    urst0h -  unload/reload device, format is: HP (200GB)
    rst0a  -  rewind device,        format is: HP (400GB w/comp)
    nrst0a -  no rewind device,     format is: HP (400GB w/comp)
    urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

A lista a seguir descreve as abreviaturas no exemplo anterior:

- GB—Gigabytes; esta é a capacidade da fita.
- w/comp—com compressão; isto mostra a capacidade da fita com compressão.

Número suportado de dispositivos de fita simultâneos

O ONTAP suporta um máximo de 64 conexões simultâneas de unidade de fita, 16 trocadores médios e 16 dispositivos de bridge ou roteador para cada sistema de armazenamento (por nó) em qualquer combinação de anexos Fibre Channel, SCSI ou SAS.

As unidades de fita ou os trocadores médios podem ser dispositivos em bibliotecas de fitas físicas ou virtuais

ou em dispositivos autônomos.

Embora um sistema de armazenamento possa detetar 64 conexões de unidade de fita, o número máximo de sessões de backup e restauração que podem ser executadas simultaneamente depende dos limites de escalabilidade do mecanismo de backup.

Informações relacionadas

Limites de escalabilidade para sessões de backup e restauração de despejo

Aliasing de fita

Visão geral da distorção da fita

Aliasing simplifica o processo de identificação do dispositivo. A distorção liga um nome de caminho físico (PPN) ou um número de série (SN) de uma fita ou um trocador de meio a um nome de alias persistente, mas modificável.

A tabela a seguir descreve como a distorção de fita permite garantir que uma unidade de fita (ou biblioteca de fitas ou trocador de médio) esteja sempre associada a um único nome de alias:

Cenário	Reatribuir o alias
Quando o sistema reinicia	A unidade de fita é reatribuída automaticamente seu alias anterior.
Quando um dispositivo de fita se move para outra porta	O alias pode ser ajustado para apontar para o novo endereço.
Quando mais de um sistema utiliza um dispositivo de fita específico	O usuário pode definir o alias para ser o mesmo para todos os sistemas.

Quando você atualiza do Data ONTAP 8.1.x para Data ONTAP 8.2.x, o recurso de alias de fita do Data ONTAP 8.2.x modifica os nomes de alias de fita existentes. Nesse caso, você pode ter que atualizar os nomes de alias de fita no aplicativo de backup.

A atribuição de aliases de fita fornece uma correspondência entre os nomes lógicos dos dispositivos de backup (por exemplo, st0 ou MC1) e um nome atribuído permanentemente a uma porta, uma unidade de fita ou um trocador de Mídia.

st0 e st00 são nomes lógicos diferentes.

Nomes lógicos e números de série são usados apenas para acessar um dispositivo. Depois que o dispositivo é acessado, ele retorna todas as mensagens de erro usando o nome do caminho físico.

Existem dois tipos de nomes disponíveis para a distorção: Nome do caminho físico e número de série.

Quais são os nomes de caminhos físicos

Nomes de caminho físico (PPNs) são as sequências de endereços numéricos que o

ONTAP atribui a unidades de fita e bibliotecas de fitas com base no adaptador ou switch SCSI-2/3 (local específico) que estão conetados ao sistema de armazenamento. PPNs também são conhecidos como nomes elétricos.

Os PPNs de dispositivos com conexão direta usam o seguinte formato `host_adapter:.device_id_lun`

> O valor LUN é exibido apenas para dispositivos de troca de fita e médio cujos valores de LUN não são zero; ou seja, se o valor LUN for zero, a `lun` parte do PPN não é exibida.

Por exemplo, o PPN 8,6 indica que o número do adaptador host é 8, o ID do dispositivo é 6 e o número da unidade lógica (LUN) é 0.

Os dispositivos de fita SAS também são dispositivos de conexão direta. Por exemplo, o PPN 5c.4 indica que em um sistema de armazenamento, o HBA SAS está conetado no slot 5, a fita SAS está conetada à porta C do HBA SAS e o ID do dispositivo é 4.

Os PPNs de dispositivos conetados a switch Fibre Channel usam o seguinte formato `switch:port_id:.device_id_lun`

Por exemplo, o PPN my_SWITCH:5.3L2 indica que a unidade de fita conetada à porta 5 de um switch chamado MY_SWITCH está definida com ID de dispositivo 3 e tem o LUN 2.

O LUN (número de unidade lógica) é determinado pela unidade. Fibre Channel, unidades de fita SCSI e bibliotecas e discos têm PPNs.

Os PPNs de unidades de fita e bibliotecas não mudam a menos que o nome do switch mude, a unidade de fita ou a biblioteca se mova ou a unidade de fita ou a biblioteca seja reconfigurada. Os PPNs permanecem inalterados após a reinicialização. Por exemplo, se uma unidade de fita chamada MY_SWITCH:5.3L2 for removida e uma nova unidade de fita com o mesmo ID de dispositivo e LUN estiver conetada à porta 5 do switch my_SWITCH, a nova unidade de fita será acessível usando MY_SWITCH:5.3L2.

Quais são os números de série

Um número de série (SN) é um identificador exclusivo para uma unidade de fita ou um carregador médio. O ONTAP gera aliases baseados no SN em vez do WWN.

Como o SN é um identificador exclusivo para uma unidade de fita ou um trocador de médio, o alias permanece o mesmo independentemente dos caminhos de conexão múltiplos para a unidade de fita ou trocador de médio. Isso ajuda os sistemas de armazenamento a rastrear a mesma unidade de fita ou carregador médio em uma configuração de biblioteca de fitas.

O SN de uma unidade de fita ou de um trocador de médio não muda mesmo se você renomear o switch Fibre Channel ao qual a unidade de fita ou o trocador de médio está conetado. No entanto, em uma biblioteca de fitas, se você substituir uma unidade de fita existente por uma nova, o ONTAP gera novos aliases porque o SN da unidade de fita muda. Além disso, se você mover uma unidade de fita existente para um novo slot em uma biblioteca de fitas ou remapear o LUN da unidade de fita, o ONTAP gera um novo alias para essa unidade de fita.

> Você deve atualizar os aplicativos de backup com os aliases recém-gerados.

O SN de um dispositivo de fita usa o seguinte formato: `SN[xxxxxxxxxx]L[X]`

x É um caractere alfanumérico e Lx é o LUN do dispositivo de fita. Se o LUN for 0, a parte Lx da cadeia de carateres não será exibida.

Cada SN é composto por até 32 carateres; o formato para o SN não é sensível a maiúsculas e minúsculas.

Considerações ao configurar o acesso à fita multipath

Você pode configurar dois caminhos do sistema de armazenamento para acessar as unidades de fita em uma biblioteca de fitas. Se um caminho falhar, o sistema de armazenamento pode usar os outros caminhos para acessar as unidades de fita sem ter que reparar imediatamente o caminho com falha. Isso garante que as operações de fita possam ser reiniciadas.

Você deve considerar o seguinte ao configurar o acesso à fita multipath a partir do seu sistema de storage:

- Em bibliotecas de fitas que suportam mapeamento LUN, para acesso multipath a um grupo LUN, o mapeamento LUN deve ser simétrico em cada caminho.

  As unidades de fita e os modificadores de Mídia são atribuídos a grupos LUN (conjunto de LUNs que compartilham o mesmo conjunto de caminhos do iniciador) em uma biblioteca de fitas. Todas as unidades de fita de um grupo LUN devem estar disponíveis para operações de backup e restauração em todos os vários caminhos.

- Um máximo de dois caminhos pode ser configurado a partir do sistema de armazenamento para acessar as unidades de fita em uma biblioteca de fitas.
- O acesso à fita multipath é compatível com o balanceamento de carga. O balanceamento de carga está desativado por padrão.

No exemplo a seguir, o sistema de armazenamento acessa o grupo LUN 0 através de dois caminhos de iniciador: 0B e 0d. Em ambos os caminhos, o grupo LUN tem o mesmo número de LUN, 0 e contagem de LUN, 5. O sistema de armazenamento acede ao grupo LUN 1 através de apenas um caminho de iniciador, 3D.

```
STSW-3070-2_cluster::> storage tape library config show

Node                    LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Para obter mais informações, consulte as páginas de manual.

Como você adiciona unidades de fita e bibliotecas aos sistemas de armazenamento

Você pode adicionar unidades de fita e bibliotecas ao sistema de armazenamento dinamicamente (sem colocar o sistema de armazenamento offline).

Quando você adiciona um novo trocador médio, o sistema de armazenamento deteta sua presença e adiciona-a à configuração. Se o trocador de meio já estiver referenciado nas informações de alias, não serão criados novos nomes lógicos. Se a biblioteca não for referenciada, o sistema de armazenamento cria um novo alias para o trocador de médio.

Em uma configuração de biblioteca de fitas, você deve configurar uma unidade de fita ou um carregador médio no LUN 0 de uma porta de destino para o ONTAP descobrir todos os trocadores médios e unidades de fita nessa porta de destino.

Quais são as reservas de fita

Vários sistemas de armazenamento podem compartilhar o acesso a unidades de fita, trocadores médios, pontes ou bibliotecas de fitas. As reservas de fita garantem que apenas um sistema de armazenamento acesse um dispositivo em qualquer momento específico, ativando o mecanismo de reserva/Liberação SCSI ou as reservas persistentes SCSI para todas as unidades de fita, trocadores médios, bridges e bibliotecas de fitas.

> Todos os sistemas que compartilham dispositivos em uma biblioteca, independentemente de os switches estarem envolvidos ou não, devem usar o mesmo método de reserva.

O mecanismo de reserva/Liberação SCSI para reservar dispositivos funciona bem em condições normais. No entanto, durante os procedimentos de recuperação de erros de interface, as reservas podem ser perdidas. Se isso ocorrer, iniciadores que não o proprietário reservado podem acessar o dispositivo.

As reservas feitas com SCSI Persistent Reservations não são afetadas por mecanismos de recuperação de erros, como restauração de loop ou restauração de destino; no entanto, nem todos os dispositivos implementam as reservas persistentes SCSI corretamente.

Transfira dados usando ndmpcopy

Transfira dados usando a visão geral do ndmpcopy

O `ndmpcopy` comando nodeshell transfere dados entre sistemas de storage que suportam o NDMP v4. Você pode realizar transferências de dados completas e incrementais. Você pode transferir volumes completos ou parciais, qtrees, diretórios ou arquivos individuais.

Sobre esta tarefa

Usando o ONTAP 8.x e versões anteriores, as transferências incrementais são limitadas a um máximo de dois níveis (um total e até dois backups incrementais).

A partir do ONTAP 9.0 e versões posteriores, as transferências incrementais são limitadas a um máximo de nove níveis (um backup completo e até nove backups incrementais).

Você pode executar `ndmpcopy` na linha de comando nodeshell dos sistemas de armazenamento de origem e

destino, ou um sistema de armazenamento que não seja a origem nem o destino da transferência de dados. Você também pode executar `ndmpcopy` em um único sistema de armazenamento que seja a origem e o destino da transferência de dados.

Você pode usar endereços IPv4 ou IPv6 dos sistemas de armazenamento de origem e destino no `ndmpcopy` comando. O formato do caminho é `/vserver_name/volume_name \[path\]`.

Passos

1. Habilite o serviço NDMP nos sistemas de storage de origem e destino:

Se estiver a efetuar a transferência de dados na origem ou destino em…	Use o seguinte comando…
Modo NDMP com escopo SVM	`vserver services ndmp on` Para autenticação NDMP no SVM admin, a conta de usuário é e a função de usuário `admin` é `admin` ou `backup`. No data SVM, a conta de usuário é `vsadmin` e a função de usuário é `vsadmin` ou `vsadmin-backup` função.
Modo NDMP com escopo de nó	`system services ndmp on`

2. Transfira dados dentro de um sistema de armazenamento ou entre sistemas de armazenamento usando o `ndmpcopy` comando no nodeshell:

`::> system node run -node <node_name> < ndmpcopy [options] source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-mcd {inet|inet6}] [-md {inet|inet6}]`

Nomes DNS não são suportados no ndmpcopy. Você deve fornecer o endereço IP da origem e do destino. O endereço de loopback (127,0.0,1) não é suportado para o endereço IP de origem ou o endereço IP de destino.

- O `ndmpcopy` comando determina o modo de endereço para conexões de controle da seguinte forma:
  - O modo de endereço para conexão de controle corresponde ao endereço IP fornecido.
  - Você pode substituir essas regras usando as `-mcs` opções e. `-mcd`
- Se a origem ou o destino for o sistema ONTAP, então, dependendo do modo NDMP (com escopo de nó ou escopo SVM), use um endereço IP que permita acesso ao volume de destino.
- `source_path` e `destination_path` são os nomes de caminho absolutos até o nível granular de volume, qtree, diretório ou arquivo.
- `-mcs` especifica o modo de endereçamento preferido para a conexão de controle ao sistema de armazenamento de origem.

  `inet` Indica um modo de endereço IPv4 e `inet6` indica um modo de endereço IPv6.

- `-mcd` especifica o modo de endereçamento preferido para a conexão de controle ao sistema de armazenamento de destino.

  `inet` Indica um modo de endereço IPv4 e `inet6` indica um modo de endereço IPv6.

- `-md` especifica o modo de endereçamento preferido para transferências de dados entre os sistemas de armazenamento de origem e destino.

  `inet` Indica um modo de endereço IPv4 e `inet6` indica um modo de endereço IPv6.

  Se você não usar a `-md` opção no `ndmpcopy` comando, o modo de endereçamento para a conexão de dados é determinado da seguinte forma:

  - Se um dos endereços especificados para as conexões de controle for um endereço IPv6, o modo de endereço para a conexão de dados é IPv6.
  - Se ambos os endereços especificados para as conexões de controle forem endereços IPv4, o `ndmpcopy` comando tentará primeiro um modo de endereço IPv6 para a conexão de dados.

    Se isso falhar, o comando usará um modo de endereço IPv4.

    Um endereço IPv6, se especificado, deve estar entre colchetes.

    Este comando de exemplo migra dados de um caminho de (`source_path`origem) para um caminho de (`destination_path`destino).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
Este comando de exemplo define explicitamente as conexões de controle e a conexão de dados para usar o modo de endereço IPv6:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Opções para o comando ndmpcopy

Você deve entender as opções disponíveis para o `ndmpcopy` comando nodeshell para transferir dados com sucesso.

A tabela a seguir lista as opções disponíveis. Para obter mais informações, consulte as `ndmpcopy` páginas de manual disponíveis através do nodeshell.

Opção	Descrição
`-sa username[password: ]`	Esta opção define o nome de usuário de autenticação de origem e a senha para conexão com o sistema de armazenamento de origem. Esta é uma opção obrigatória. Para um usuário sem privilégio de administrador, você deve especificar a senha específica do NDMP gerada pelo sistema do usuário. A senha gerada pelo sistema é obrigatória para usuários admin e não admin.
`-da username[password: ]`	Esta opção define o nome de utilizador e a palavra-passe de autenticação de destino para ligação ao sistema de armazenamento de destino. Esta é uma opção obrigatória.
`-st {md5`	`text`Selecione
Esta opção define o tipo de autenticação de origem a ser usado ao se conetar ao sistema de armazenamento de origem. Esta é uma opção obrigatória e, portanto, o usuário deve fornecer a `text` opção ou `md5`.	`-dt {md5`
`text`Selecione	Esta opção define o tipo de autenticação de destino a ser usado ao se conetar ao sistema de armazenamento de destino.
`-l`	Esta opção define o nível de despejo usado para a transferência para o valor especificado de level.valid values are `0 1` , , to `9`, where `0` indica uma transferência completa e `1 9` especifica uma transferência incremental. A predefinição é `0`.
`-d`	Esta opção permite a geração de mensagens de log de depuração ndmpcopy. Os arquivos de log de depuração do ndmpcopy estão localizados no `/mroot/etc/log` volume raiz. Os nomes dos arquivos de log de depuração do ndmpcopy estão no `ndmpcopy.yyyymmdd` formato.
`-f`	Esta opção ativa o modo forçado. Este modo permite que os arquivos do sistema sejam sobrescritos no `/etc` diretório na raiz do volume do 7-Mode.
`-h`	Esta opção imprime a mensagem de ajuda.

Opção	Descrição
`-p`	Esta opção solicita que você insira a senha para autorização de origem e destino. Esta palavra-passe substitui a palavra-passe especificada para `-sa` as opções e. `-da` Você pode usar essa opção somente quando o comando estiver sendo executado em um console interativo.
`-exclude`	Esta opção exclui arquivos ou diretórios especificados do caminho especificado para transferência de dados. O valor pode ser uma lista separada por vírgulas de nomes de diretórios ou arquivos, como **`.pst`** `.txt` ou .

NDMP para volumes FlexVol

Sobre o NDMP para volumes FlexVol

O Network Data Management Protocol (NDMP) é um protocolo padronizado para controle de backup, recuperação e outros tipos de transferência de dados entre dispositivos de armazenamento primário e secundário, como sistemas de armazenamento e bibliotecas de fitas.

Ao ativar o suporte NDMP em um sistema de armazenamento, você permite que esse sistema de armazenamento se comunique com aplicativos de backup conetados à rede habilitados para NDMP (também chamados de *Data Management Applications* ou *DMAs*), servidores de dados e servidores de fita participantes de operações de backup ou recuperação. Todas as comunicações de rede ocorrem através da rede TCPIP ou TCP/IPv6. O NDMP também fornece controle de baixo nível de unidades de fita e trocadores médios.

Você pode executar operações de backup em fita e restauração no modo NDMP com escopo de nó ou no modo NDMP com escopo de máquina virtual de armazenamento (SVM).

Você deve estar ciente das considerações que você deve levar em conta ao usar NDMP, lista de variáveis de ambiente e topologias de backup em fita NDMP compatíveis. Você também pode ativar ou desativar a funcionalidade DAR aprimorada. Os dois métodos de autenticação suportados pelo ONTAP para autenticar o acesso NDMP a um sistema de armazenamento são: Texto simples e desafio.

Informações relacionadas

Variáveis de ambiente suportadas pelo ONTAP

Sobre os modos de operação NDMP

Sobre os modos de operação NDMP

Você pode optar por realizar backup em fita e restaurar operações no nível do nó ou no nível da máquina virtual de storage (SVM). Para realizar essas operações com sucesso

no nível do SVM, o serviço NDMP precisa estar habilitado no SVM.

Se você atualizar do Data ONTAP 8.2 para o Data ONTAP 8.3, o modo de operação NDMP usado no 8,2 continuará sendo mantido após a atualização de 8,2 para 8,3.

Se você instalar um novo cluster com o Data ONTAP 8.2 ou posterior, o NDMP estará no modo NDMP com escopo SVM por padrão. Para executar operações de backup e restauração de fita no modo NDMP com escopo de nó, você deve ativar explicitamente o modo NDMP com escopo de nó.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo de nó

Gerenciamento do modo NDMP com escopo de nó para volumes FlexVol

Gerenciamento do modo NDMP com escopo da SVM para volumes FlexVol

Qual é o modo NDMP com escopo de nó

No modo NDMP com escopo de nó, você pode executar operações de backup em fita e restauração no nível do nó. O modo NDMP de operação usado no Data ONTAP 8.2 continuará sendo mantido após a atualização de 8,2 para 8,3.

No modo NDMP com escopo de nó, você pode executar operações de backup em fita e restauração em um nó que possua o volume. Para executar essas operações, você deve estabelecer conexões de controle NDMP em um LIF hospedado no nó que possui o volume ou os dispositivos de fita.

Este modo está obsoleto e será removido em uma futura versão principal.

Informações relacionadas

Gerenciamento do modo NDMP com escopo de nó para volumes FlexVol

Qual é o modo NDMP com escopo SVM

Você pode executar com êxito as operações de backup em fita e restauração no nível da máquina virtual de storage (SVM) se o serviço NDMP estiver habilitado no SVM. Você pode fazer backup e restaurar todos os volumes hospedados em diferentes nós na SVM de um cluster, se a aplicação de backup suportar a EXTENSÃO CAB.

Uma conexão de controle NDMP pode ser estabelecida em diferentes tipos de LIF. No modo NDMP com escopo da SVM, esses LIFs pertencem ao data SVM ou admin SVM. A conexão pode ser estabelecida em um LIF somente se o serviço NDMP estiver habilitado no SVM que possui esse LIF.

Um LIF de dados pertence ao data SVM e o LIF entre clusters, LIF de gerenciamento de nós e LIF de clusters pertencem ao administrador SVM.

No modo NDMP com escopo SVM, a disponibilidade de volumes e dispositivos de fita para operações de backup e restauração depende do tipo de LIF no qual a conexão de controle NDMP é estabelecida e do status da extensão DA CABINE. Se o aplicativo de backup suportar a EXTENSÃO CAB e um volume e o dispositivo de fita compartilharem a mesma afinidade, o aplicativo de backup poderá executar uma operação de backup ou restauração local, em vez de uma operação de backup ou restauração de três vias.

Informações relacionadas

Considerações ao usar NDMP

Você precisa levar em conta várias considerações ao iniciar o serviço NDMP no sistema de storage.

- Cada nó dá suporte a um máximo de 16 backups, restaurações ou combinações simultâneos dos dois usando unidades de fita conetadas.
- Os serviços NDMP podem gerar dados do histórico de arquivos a pedido de aplicativos de backup NDMP.

  O histórico de arquivos é usado por aplicativos de backup para permitir a recuperação otimizada de subconjuntos de dados selecionados de uma imagem de backup. A geração e o processamento do histórico de arquivos podem consumir muito tempo e uso intenso de CPU para o sistema de storage e para o aplicativo de backup.

  SMTape não suporta histórico de arquivos.

  Se sua proteção de dados estiver configurada para recuperação de desastres - onde toda a imagem de backup será recuperada - você pode desativar a geração do histórico de arquivos para reduzir o tempo de backup. Consulte a documentação do aplicativo de backup para determinar se é possível desativar a geração do histórico de arquivos NDMP.

- A política de firewall para NDMP é ativada por padrão em todos os tipos de LIF.
- No modo NDMP com escopo de nó, o backup de um FlexVol volume requer que você use o aplicativo de backup para iniciar um backup em um nó que possua o volume.

  No entanto, não é possível fazer backup de um volume raiz de nó.

- Você pode executar backup NDMP de qualquer LIF conforme permitido pelas políticas de firewall.

  Se você usar um LIF de dados, deverá selecionar um LIF que não esteja configurado para failover. Se um LIF de dados falhar durante uma operação NDMP, a operação NDMP falhará e deverá ser executada novamente.

- No modo NDMP com escopo de nó e no modo NDMP com escopo de máquina virtual de armazenamento (SVM) sem suporte de extensão DE CAB, a conexão de dados NDMP usa o mesmo LIF da conexão de controle NDMP.
- Durante a migração de LIF, as operações de backup e restauração contínuas são interrompidas.

  Você deve iniciar as operações de backup e restauração após a migração de LIF.

- O caminho de backup NDMP é do formato */vserver_name/volume_name/path_name*.

  path_name É opcional e especifica o caminho do diretório, arquivo ou cópia Snapshot.

- Quando um destino SnapMirror é feito backup em fita usando o mecanismo de despejo, apenas os dados no volume são copiados.

  No entanto, se um destino SnapMirror for feito backup em fita usando SMTape, os metadados também serão copiados. As relações do SnapMirror e os metadados associados não são copiados para a fita. Portanto, durante a restauração, apenas os dados nesse volume são restaurados, mas as relações SnapMirror associadas não são restauradas.

Informações relacionadas

O que a extensão Cluster Aware Backup faz

"Administração do sistema"

Variável de ambiente

Visão geral das variáveis de ambiente

As variáveis de ambiente são usadas para comunicar informações sobre uma operação de backup ou restauração entre um aplicativo de backup habilitado para NDMP e um sistema de armazenamento.

Por exemplo, se um usuário especificar que um aplicativo de backup deve fazer `/vserver1/vol1/dir1` backup , o aplicativo de backup define a variável de ambiente DO SISTEMA DE ARQUIVOS como `/vserver1/vol1/dir1`. Da mesma forma, se um usuário especificar que um backup deve ser um backup de nível 1, o aplicativo de backup define a variável de ambiente de NÍVEL como 1 (um).

> A configuração e a análise de variáveis de ambiente são geralmente transparentes para os administradores de backup, ou seja, o aplicativo de backup as define automaticamente.

Um administrador de backup raramente especifica variáveis de ambiente; no entanto, você pode querer alterar o valor de uma variável de ambiente daquele definido pelo aplicativo de backup para caraterizar ou contornar um problema funcional ou de desempenho. Por exemplo, um administrador pode querer desativar temporariamente a geração do histórico de arquivos para determinar se o processamento de informações do histórico de arquivos do aplicativo de backup está contribuindo para problemas de desempenho ou problemas funcionais.

Muitos aplicativos de backup fornecem um meio de substituir ou modificar variáveis de ambiente ou especificar variáveis de ambiente adicionais. Para obter informações, consulte a documentação do aplicativo de backup.

Variáveis de ambiente suportadas pelo ONTAP

As variáveis de ambiente são usadas para comunicar informações sobre uma operação de backup ou restauração entre um aplicativo de backup habilitado para NDMP e um sistema de armazenamento. O ONTAP suporta variáveis de ambiente, que têm um valor padrão associado. No entanto, você pode modificar manualmente esses valores padrão.

Se você modificar manualmente os valores definidos pelo aplicativo de backup, o aplicativo pode se comportar de forma imprevisível. Isso ocorre porque as operações de backup ou restauração podem não estar fazendo o que o aplicativo de backup esperava que fizessem, mas em alguns casos, a modificação criteriosa pode ajudar a identificar ou solucionar problemas.

As tabelas a seguir listam as variáveis de ambiente cujo comportamento é comum para dump e SMTape e aquelas variáveis que são suportadas apenas para dump e SMTape. Essas tabelas também contêm descrições de como as variáveis de ambiente que são suportadas pelo ONTAP funcionam se forem usadas:

> Na maioria dos casos, variáveis que têm o valor, `Y` também aceitam `T` e `N` também aceitam `F`.

Variáveis de ambiente suportadas para dump e SMTape

Variável de ambiente	Valores válidos	Padrão	Descrição
DEPURAR	`Y` ou `N`	`N`	Especifica que as informações de depuração são impressas.
SISTEMA DE FICHEIROS	`string`	`none`	Especifica o nome do caminho da raiz dos dados que estão sendo copiados.
NDMP_VERSION	`return_only`	`none`	Você não deve modificar a variável NDMP_VERSION. Criada pela operação de backup, a variável NDMP_VERSION retorna a versão NDMP. O ONTAP define a variável NDMP_VERSION durante um backup para uso interno e para passar para um aplicativo de backup para fins informativos. A versão NDMP de uma sessão NDMP não é definida com esta variável.
PATHNAME_SEPARATOR	`return_value`	`none`	Especifica o caractere separador do nome do caminho. Este caractere depende do backup do sistema de arquivos. Para ONTAP, o caractere "'/'" é atribuído a essa variável. O servidor NDMP define essa variável antes de iniciar uma operação de backup em fita.

Variável de ambiente	Valores válidos	Padrão	Descrição
TIPO	`dump` ou `smtape`	`dump`	Especifica o tipo de backup suportado para executar operações de backup e restauração em fita.
VERBOSO	`Y` ou `N`	`N`	Aumenta as mensagens de log durante a execução de uma operação de backup ou restauração de fita.

Variáveis de ambiente suportadas para dump

Variável de ambiente	Valores válidos	Padrão	Descrição
ACL_START	`return_only`	`none`	Criada pela operação de backup, a variável ACL_START é um valor de deslocamento usado por uma restauração de acesso direto ou operação de backup NDMP reiniciável. O valor de deslocamento é o deslocamento de byte no arquivo de despejo onde os dados ACL (passe V) começam e são retornados no final de um backup. Para que uma operação de restauração de acesso direto restaure corretamente os dados de backup, o valor ACL_START deve ser passado para a operação de restauração quando ela for iniciada. Uma operação de backup NDMP reiniciável usa o valor ACL_START para se comunicar com o aplicativo de backup onde a parte não reiniciável do fluxo de backup começa.

Variável de ambiente	Valores válidos	Padrão	Descrição
DATA_BASE	`0`, `-1`, ou `DUMP_DATE` valor	`-1`	Especifica a data de início para backups incrementais. Quando definido como `-1`, o especificador incremental BASE_DATE é desativado. Quando definido como `0` em um backup de nível 0, backups incrementais são ativados. Após o backup inicial, o valor da variável DUMP_DATE do backup incremental anterior é atribuído à variável BASE_DATE. Essas variáveis são uma alternativa aos backups incrementais baseados em NÍVEL/ATUALIZAÇÃO.
DIRETA	`Y` ou `N`	`N`	Especifica que uma restauração deve avançar rapidamente diretamente para o local na fita onde os dados do arquivo residem, em vez de digitalizar toda a fita. Para que a recuperação de acesso direto funcione, o aplicativo de backup deve fornecer informações de posicionamento. Se essa variável estiver definida como `Y`, o aplicativo de backup especificará os nomes de arquivo ou diretório e as informações de posicionamento.

Variável de ambiente	Valores válidos	Padrão	Descrição
NOME_DMP	`string`	`none`	Especifica o nome para um backup de várias subárvores. Esta variável é obrigatória para múltiplos backups de subárvore.
DUMP_DATE	`return_value`	`none`	Você não altera essa variável diretamente. Ele é criado pelo backup se a variável BASE_DATE for definida como um valor diferente `-1`de . A variável DUMP_DATE é derivada pela prependência do valor de nível de 32 bits para um valor de tempo de 32 bits calculado pelo software dump. O nível é incrementado a partir do último valor de nível passado para a variável BASE_DATE. O valor resultante é usado como o valor BASE_DATE em um backup incremental subsequente.

Variável de ambiente	Valores válidos	Padrão	Descrição
ENHANCED_DAR_ENABLED (MELHORADO_DAR_ATIVADO	`Y` ou `N`	`N`	Especifica se a funcionalidade DAR aprimorada está ativada. A FUNCIONALIDADE DAR aprimorada suporta DAR de diretório e DAR de arquivos com fluxos NT. Ele fornece melhorias de desempenho. DAR aprimorado durante a restauração só é possível se as seguintes condições forem atendidas: • ONTAP suporta DAR melhorado. • O histórico do ficheiro está ativado durante a cópia de segurança. • A `ndmpd.offset_map.enable` opção está definida como `on`. • ENHANCED_DAR_ENABLED variável é definida como `Y` durante a restauração.

Variável de ambiente	Valores válidos	Padrão	Descrição
EXCLUIR	`pattern_string`	`none`	Especifica arquivos ou diretórios excluídos ao fazer backup de dados. A lista Excluir é uma lista separada por vírgulas de nomes de arquivo ou diretório. Se o nome de um arquivo ou diretório corresponder a um dos nomes na lista, ele será excluído do backup. As seguintes regras se aplicam ao especificar nomes na lista Excluir: • O nome exato do arquivo ou diretório deve ser usado. • O asterisco (*), um caractere curinga, deve ser o primeiro ou o último caractere da cadeia de carateres. Cada string pode ter até dois asteriscos. • Uma vírgula em um nome de arquivo ou diretório deve ser precedida por uma barra invertida. • A lista Excluir pode conter até 32 nomes. Os arquivos ou diretórios especificados para serem excluídos para backup não serão excluídos se você definir Non_QUOTA_TREE como `Y` simultaneamente.

Variável de ambiente	Valores válidos	Padrão	Descrição
EXTRAIR	`Y`, `N`, ou `E`	`N`	Especifica que subárvores de um conjunto de dados de backup devem ser restauradas. O aplicativo de backup especifica os nomes das subárvores a serem extraídas. Se um arquivo especificado corresponder a um diretório cujo conteúdo foi feito backup, o diretório é extraído recursivamente. Para renomear um arquivo, diretório ou qtree durante a restauração sem usar DAR, você deve definir a variável de ambiente EXTRAIR como `E`.
EXTRACT_ACL	`Y` ou `N`	`Y`	Especifica que as ACLs do arquivo de backup são restauradas em uma operação de restauração. O padrão é restaurar ACLs ao restaurar dados, exceto para DARS.

Variável de ambiente	Valores válidos	Padrão	Descrição
FORÇA	`Y` ou `N`	`N`	Determina se a operação de restauração deve verificar se há espaço de volume e disponibilidade de inode no volume de destino. Definir essa variável para `Y` fazer com que a operação de restauração pule as verificações de espaço de volume e disponibilidade de inode no caminho de destino. Se não houver espaço de volume suficiente ou inodes disponíveis no volume de destino, a operação de restauração recupera a quantidade de dados permitidos pelo espaço de volume de destino e pela disponibilidade de inodes. A operação de restauração pára quando o espaço de volume ou inodes não estão disponíveis.

Variável de ambiente	Valores válidos	Padrão	Descrição
HIST	`Y` ou `N`	`N`	Especifica que as informações do histórico de arquivos são enviadas para o aplicativo de backup. A maioria dos aplicativos de backup comerciais define a variável HIST como `Y`. Se quiser aumentar a velocidade de uma operação de backup ou solucionar um problema com a coleção de histórico de arquivos, defina essa variável como `N`. Não deve definir a variável HIST para `Y` se a aplicação de cópia de segurança não suportar o histórico de ficheiros.

Variável de ambiente	Valores válidos	Padrão	Descrição
IGNORE_CTIME	`Y` ou `N`	`N`	Especifica que o backup de um arquivo não é incrementalmente feito se somente seu valor ctime tiver sido alterado desde o backup incremental anterior. Alguns aplicativos, como software de verificação de vírus, alteram o valor ctime de um arquivo dentro do inode, mesmo que o arquivo ou seus atributos não tenham sido alterados. Como resultado, um backup incremental pode fazer backup de arquivos que não foram alterados. A `IGNORE_CTIME` variável deve ser especificada somente se backups incrementais estiverem tomando uma quantidade inaceitável de tempo ou espaço porque o valor ctime foi modificado. O `NDMP dump` comando define `IGNORE_CTIME` como `false` por padrão. Definir para que isso `true` possa resultar na seguinte perda de dados: 1. Se `IGNORE_CTIME` estiver definido como verdadeiro com

Variável de ambiente	Valores válidos	Padrão	Descrição
IGNORE_QTREES	`Y` ou `N`	`N`	Especifica que a operação de restauração não restaura informações de qtree de qtrees de backup.
NÍVEL	`0-31`	`0`	Especifica o nível de backup. O nível 0 copia todo o conjunto de dados. Níveis de backup incremental, especificados por valores acima de 0, copie todos os arquivos (novos ou modificados) desde o último backup incremental. Por exemplo, um nível 1 faz backup de arquivos novos ou modificados desde o backup de nível 0, um nível 2 faz backup de arquivos novos ou modificados desde o backup de nível 1 e assim por diante.
LISTA	`Y` ou `N`	`N`	Lista os nomes dos arquivos de backup e os números de inode sem realmente restaurar os dados.
LIST_QTREES	`Y` ou `N`	`N`	Lista os qtrees de backup sem realmente restaurar os dados.

exclusão de arquivos, que são movidos através de qtrees na fonte durante a restauração increm

Variável de ambiente	Valores válidos	Padrão	Descrição
MULTI_SUBTREE_ NOMES	`string`	`none`	Especifica que o backup é um backup de várias subárvores. Várias subárvores são especificadas na cadeia de carateres, que é uma lista de nomes de subárvores separada por uma nova linha. As subárvores são especificadas por nomes de caminho relativos ao seu diretório raiz comum, que deve ser especificado como o último elemento da lista. Se você usar essa variável, você também deve usar a variável DMP_NAME.
NDMP_UNICODE_ FH	`Y` ou `N`	`N`	Especifica que um nome Unicode é incluído além do nome NFS do arquivo nas informações do histórico do arquivo. Essa opção não é usada pela maioria dos aplicativos de backup e não deve ser definida a menos que o aplicativo de backup seja projetado para receber esses nomes de arquivo adicionais. A variável HIST também deve ser definida.
NO_ACLS	`Y` ou `N`	`N`	Especifica que as ACLs não devem ser copiadas ao fazer backup de dados.

Variável de ambiente	Valores válidos	Padrão	Descrição
NON_QUOTA_TREE	`Y` ou `N`	`N`	Especifica que os arquivos e diretórios no qtrees devem ser ignorados ao fazer backup de dados. Quando definido como `Y`, os itens no qtrees no conjunto de dados especificado pela variável SISTEMA DE ARQUIVOS não são copiados. Esta variável tem um efeito somente se a variável FILESYSTEM especificar um volume inteiro. A variável non_QUOTA_TREE só funciona em um backup de nível 0 e não funciona se a variável MULTI_SUBTREE_NAMES for especificada. Os arquivos ou diretórios especificados para serem excluídos para backup não serão excluídos se você definir Non_QUOTA_TREE como `Y` simultaneamente.
NOWRITE	`Y` ou `N`	`N`	Especifica que a operação de restauração não deve gravar dados no disco. Esta variável é usada para depuração.

Variável de ambiente	Valores válidos	Padrão	Descrição
RECURSIVA	`Y` ou `N`	`Y`	Especifica que as entradas de diretório durante uma restauração DAR serão expandidas. As variáveis de ambiente DIRECT e ENHANCED_DAR_ENABLED também devem estar ativadas (definidas para `Y`). Se a variável RECURSIVA estiver desativada (definida como `N`), somente as permissões e ACLs de todos os diretórios no caminho de origem original serão restauradas a partir da fita, não do conteúdo dos diretórios. Se a variável RECURSIVA estiver definida como `N` ou a variável RECOVER_full_PATHS estiver definida como `Y`, o caminho de recuperação deve terminar com o caminho original.

Variável de ambiente	Valores válidos	Padrão	Descrição
RECUPERAR_FULL_PATHS	`Y` ou `N`	`N`	Especifica que o caminho de recuperação completo terá suas permissões e ACLs restauradas após o DAR. DIRECT e ENHANCED_DAR_ENABLED também devem ser ativados (definidos como `Y`). Se RECOVER_full_PATHS estiver definido como `Y`, o caminho de recuperação deve terminar com o caminho original. Se os diretórios já existirem no volume de destino, suas permissões e ACLs não serão restaurados da fita.
ATUALIZAÇÃO	`Y` ou `N`	`Y`	Atualiza as informações de metadados para habilitar o backup incremental baseado em NÍVEL.

Variáveis de ambiente suportadas para SMTape

de erro.

Por exemplo, os seguintes são caminhos de recuperação válidos porque todos os caminhos de recuperação estão dentro `foo/dir1/deepdir/myfile`de :

- `/foo`
- `/foo/dir`
- `/foo/dir1/deepdir`
- `/foo/dir1/deepdir/myfile`

Os seguintes são caminhos de recuperação inválidos:

- `/foo`

  `/foo/dir`

  `/foo/dir1/myfile`

-
- /foo/dir2
- /foo/dir2/myfile

Variável de ambiente	Valores válidos	Padrão	Descrição
DATA_BASE	`DUMP_DATE`	`-1`	Especifica a data de início para backups incrementais. `BASE_DATE` É uma representação de cadeia de carateres dos identificadores Snapshot de referência. Usando a `BASE_DATE` cadeia de carateres, o SMTape localiza a cópia Snapshot de referência. `BASE_DATE` não é necessário para backups de linha de base. Para um backup incremental, o valor da `DUMP_DATE` variável da linha de base anterior ou backup incremental é atribuído à `BASE_DATE` variável. O aplicativo de backup atribui o `DUMP_DATE` valor de uma linha de base ou backup incremental SMTape anterior.

Variável de ambiente	Valores válidos	Padrão	Descrição
DUMP_DATE	`return_value`	`none`	No final de um backup SMTape, DUMP_DATE contém um identificador de cadeia de carateres que identifica a cópia Snapshot usada para esse backup. Esta cópia Snapshot pode ser usada como cópia Snapshot de referência para um backup incremental subsequente. O valor resultante de DUMP_DATE é usado como o valor BASE_DATE para backups incrementais subsequentes.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifica a sequência de backups incrementais associados ao backup de linha de base. O ID do conjunto de cópias de segurança é um ID exclusivo de 128 bits que é gerado durante uma cópia de segurança de linha de base. O aplicativo de backup atribui esse ID como entrada à `SMTAPE_BACKUP_SET_ID` variável durante um backup incremental.

Variável de ambiente	Valores válidos	Padrão	Descrição
SMTAPE_SNAPSHOT_NAME	Qualquer cópia Snapshot válida disponível no volume	`Invalid`	Quando a variável SMTAPE_SNAPSHOT_NAME está definida como uma cópia Snapshot, essa cópia Snapshot e suas cópias Snapshot mais antigas são feitas backup em fita. Para backup incremental, essa variável especifica a cópia Snapshot incremental. A variável BASE_DATE fornece a cópia Snapshot da linha de base.
SMTAPE_DELETE_SNAPSHOT	`Y` ou `N`	`N`	Para uma cópia Snapshot criada automaticamente pelo SMTape, quando a variável SMTAPE_DELETE_SNAPSHOT estiver definida como `Y`, depois que a operação de backup estiver concluída, o SMTape exclui essa cópia Snapshot. No entanto, uma cópia Snapshot criada pelo aplicativo de backup não será excluída.
SMTAPE_BREAK_MIRROR	`Y` ou `N`	`N`	Quando a variável SMTAPE_BREAK_MIRROR é definida como `Y`, o volume do tipo `DP` é alterado para um `RW` volume após uma restauração bem-sucedida.

Topologias comuns de backup de fita NDMP

O NDMP dá suporte a várias topologias e configurações entre aplicativos de backup e sistemas de storage ou outros servidores NDMP que fornecem dados (sistemas de arquivos) e serviços de fita.

Sistema de storage para fita local

Na configuração mais simples, um aplicativo de backup faz backup dos dados de um sistema de storage para um subsistema de fita conetado ao sistema de storage. A conexão de controle NDMP existe através do limite da rede. A conexão de dados NDMP que existe no sistema de storage entre os serviços de dados e fita é chamada de configuração local NDMP.

Sistema de storage para fita anexado a outro sistema de storage

Um aplicativo de backup também pode fazer backup de dados de um sistema de armazenamento para uma biblioteca de fitas (um trocador de médio com uma ou mais unidades de fita) conetada a outro sistema de armazenamento. Neste caso, a conexão de dados NDMP entre os serviços de dados e fita é fornecida por uma conexão de rede TCP ou TCP/IPv6. Isso é chamado de uma configuração de sistema de storage três vias NDMP para o sistema de storage.

Biblioteca de fitas conetada ao sistema de storage à rede

As bibliotecas de fitas habilitadas para NDMP fornecem uma variação da configuração de três vias. Nesse caso, a biblioteca de fitas se coneta diretamente à rede TCP/IP e se comunica com o aplicativo de backup e o sistema de armazenamento por meio de um servidor NDMP interno.

Sistema de storage para servidor de dados para fita ou servidor para sistema de storage para fita

O NDMP também dá suporte a configurações de três vias de sistema de storage para servidor de dados e servidor para storage, embora essas variantes sejam menos amplamente implantadas. O sistema de armazenamento para servidor permite o backup de dados do sistema de armazenamento em uma biblioteca de fitas conetada ao host do aplicativo de backup ou a outro sistema de servidor de dados. A configuração do sistema de servidor para armazenamento permite que os dados do servidor sejam copiados para uma biblioteca de fitas conetada ao sistema de armazenamento.

Métodos de autenticação NDMP compatíveis

Você pode especificar um método de autenticação para permitir solicitações de conexão NDMP. O ONTAP oferece suporte a dois métodos para autenticar o acesso NDMP a um sistema de storage: Texto simples e desafio.

No modo NDMP com escopo de nó, desafio e texto sem formatação são ativados por padrão. No entanto, você não pode desativar o desafio. Você pode ativar e desativar texto sem formatação. No método de autenticação em texto simples, a senha de login é transmitida como texto não criptografado.

No modo NDMP com escopo de máquina virtual de storage (SVM), por padrão o método de autenticação é um desafio. Ao contrário do modo NDMP com escopo de nó, neste modo você pode ativar e desativar métodos de autenticação de texto simples e desafio.

Informações relacionadas

Autenticação de usuário em um modo NDMP com escopo de nó

Autenticação de usuário no modo NDMP com escopo SVM

Extensões NDMP suportadas por ONTAP

O NDMP v4 fornece um mecanismo para criar extensões de protocolo NDMP v4 sem modificar o protocolo principal do NDMP v4. Você deve estar ciente das extensões NDMP v4 que são suportadas pelo ONTAP.

As seguintes extensões NDMP v4 são suportadas pelo ONTAP:

- Backup ciente de cluster (CAB)

  Essa extensão só é suportada no modo NDMP com escopo SVM.

- Extensão de endereço de conexão (CAE) para suporte a IPv6
- Classe de extensão 0x2050

  Essa extensão suporta operações de backup reiniciáveis e extensões de gerenciamento de Snapshot.

  A `NDMP_SNAP_RECOVER` mensagem, que faz parte das Extensões de Gerenciamento de Snapshot, é usada para iniciar uma operação de recuperação e transferir os dados recuperados de uma cópia Snapshot local para um local do sistema de arquivos local. No ONTAP, esta mensagem permite a recuperação de volumes e arquivos regulares apenas.

  ```
  `NDMP_SNAP_DIR_LIST`A mensagem permite que você navegue pelas cópias Snapshot de um volume. Se uma operação sem interrupções ocorrer enquanto uma operação de navegação estiver em andamento, o aplicativo de backup deverá reiniciar a operação de navegação.
  ```

Extensão de backup NDMP restartable para um despejo suportado pelo ONTAP

Você pode usar a funcionalidade de extensão de backup reiniciável NDMP (RBE) para reiniciar um backup a partir de um ponto de verificação conhecido no fluxo de dados antes da falha.

O que é a funcionalidade DAR melhorada

Você pode usar a funcionalidade avançada de recuperação de acesso direto (DAR) para DAR de diretório e DAR de arquivos e fluxos NT. Por padrão, a funcionalidade DAR aprimorada está ativada.

A ativação da FUNCIONALIDADE DAR aprimorada pode afetar o desempenho do backup porque um mapa de deslocamento precisa ser criado e gravado em fita. Você pode ativar ou desativar O DAR aprimorado nos modos NDMP com escopo de nó e máquina virtual de armazenamento (SVM).

Limites de escalabilidade para sessões NDMP

Você deve estar ciente do número máximo de sessões NDMP que podem ser estabelecidas simultaneamente em sistemas de armazenamento de diferentes capacidades de memória do sistema. Este número máximo depende da memória do sistema de um sistema de armazenamento.

Os limites mencionados na tabela a seguir são para o servidor NDMP. Os limites mencionados na seção "limites de escalabilidade para sessões de backup e restauração de despejo" são para a sessão de despejo e restauração.

Limites de escalabilidade para sessões de backup e restauração de despejo

Memória do sistema de um sistema de armazenamento	Número máximo de sessões NDMP
Menos de 16 GB	8
Maior ou igual a 16 GB, mas inferior a 24 GB	20
Maior ou igual a 24 GB	36

Você pode obter a memória do sistema do seu sistema de armazenamento usando o `sysconfig -a` comando (disponível através do nodeshell). Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Sobre o NDMP para volumes FlexGroup

A partir do ONTAP 9.7, o NDMP é compatível com volumes FlexGroup.

A partir do ONTAP 9.7, o comando ndmpcopy é suportado para transferência de dados entre volumes FlexVol e FlexGroup.

Se você reverter do ONTAP 9.7 para uma versão anterior, as informações de transferência incremental das transferências anteriores não serão mantidas e, portanto, você deverá executar uma cópia de linha de base após reverter.

A partir do ONTAP 9.8, os seguintes recursos NDMP são compatíveis com volumes FlexGroup:

- A mensagem NDMP_snap_RECOVER na classe de extensão 0x2050 pode ser usada para recuperar arquivos individuais em um volume FlexGroup.
- A extensão de backup reiniciável (RBE) NDMP é compatível com volumes FlexGroup.
- As variáveis de ambiente EXCLUEM e MULTI_SUBTREE_NAMES são suportadas para volumes FlexGroup.

Sobre o NDMP com SnapLock volumes

A criação de várias cópias de dados regulamentados proporciona cenários de recuperação redundantes. Com o uso de despejo e restauração NDMP, é possível preservar as características WORM (write once, read many) dos arquivos de origem em um volume SnapLock.

Os atributos DO WORM nos arquivos em um volume SnapLock são preservados ao fazer backup, restaurar e copiar dados; no entanto, atributos WORM são aplicados apenas ao restaurar para um volume SnapLock. Se um backup de um volume SnapLock for restaurado para um volume diferente de um volume SnapLock, os atributos WORM serão preservados, mas serão ignorados e não serão aplicados pelo ONTAP.

Gerenciar o modo NDMP com escopo de nó para volumes FlexVol

Gerencie o modo NDMP com escopo de nó para visão geral do FlexVol volumes

Você pode gerenciar NDMP no nível do nó usando opções e comandos NDMP. Você pode modificar as opções NDMP usando o `options` comando. Você deve usar credenciais específicas do NDMP para acessar um sistema de storage para executar operações de backup e restauração em fita.

Para obter mais informações sobre o `options` comando, consulte as páginas de manual.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo de nó

Qual é o modo NDMP com escopo de nó

Comandos para gerenciar o modo NDMP com escopo de nó

Você pode usar os `system services ndmp` comandos para gerenciar NDMP em um nível de nó. Alguns desses comandos são obsoletos e serão removidos em uma futura versão principal.

Você pode usar os seguintes comandos NDMP somente no nível avançado de privilégio:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Se você quiser…	Use este comando…
Ativar o serviço NDMP	`system services ndmp on*`
Desativar o serviço NDMP	`system services ndmp off*`
Apresentar a configuração NDMP	`system services ndmp show*`
Modificar a configuração NDMP	`system services ndmp modify*`
Exibir a versão padrão do NDMP	`system services ndmp version*`
Exibir a configuração do serviço NDMP	`system services ndmp service show`
Modificar a configuração do serviço NDMP	`system services ndmp service modify`
Exibir todas as sessões NDMP	`system services ndmp status`

Se você quiser…	Use este comando…
Exibir informações detalhadas sobre todas as sessões NDMP	`system services ndmp probe`
Termine a sessão NDMP especificada	`system services ndmp kill`
Encerrar todas as sessões NDMP	`system services ndmp kill-all`
Altere a senha NDMP	`system services ndmp password*`
Ative o modo NDMP com escopo de nó	`system services ndmp node-scope-mode on*`
Desative o modo NDMP com escopo de nó	`system services ndmp node-scope-mode off*`
Exibir o status do modo NDMP com escopo do nó	`system services ndmp node-scope-mode status*`
Encerrar com força todas as sessões NDMP	`system services ndmp service terminate`
Inicie o daemon de serviço NDMP	`system services ndmp service start`
Pare o daemon de serviço NDMP	`system services ndmp service stop`
Inicie o registo para a sessão NDMP especificada	`system services ndmp log start*`
Parar o registo para a sessão NDMP especificada	`system services ndmp log stop*`

- Esses comandos são obsoletos e serão removidos em uma futura versão principal.

Para obter mais informações sobre esses comandos, consulte as páginas de manual dos `system services ndmp` comandos.

Autenticação de usuário em um modo NDMP com escopo de nó

No modo NDMP com escopo de nó, você deve usar credenciais específicas do NDMP para acessar um sistema de storage para executar operações de backup e restauração de fita.

O ID de usuário padrão é "root". Antes de usar o NDMP em um nó, você deve garantir que você altere a senha padrão do NDMP associada ao usuário NDMP. Você também pode alterar o ID de usuário NDMP padrão.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo de nó

Gerenciar o modo NDMP com escopo SVM para volumes FlexVol

Gerenciar o modo NDMP com escopo SVM para visão geral do FlexVol volumes

Você pode gerenciar NDMP por SVM usando as opções e comandos NDMP. Você pode modificar as opções NDMP usando o `vserver services ndmp modify` comando. No modo NDMP com escopo SVM, a autenticação do usuário é integrada ao mecanismo de controle de acesso baseado em funções.

Você pode adicionar NDMP na lista de protocolos permitidos ou não permitidos usando o `vserver modify` comando. Por padrão, NDMP está na lista de protocolos permitidos. Se NDMP for adicionado à lista de protocolos não permitidos, as sessões NDMP não poderão ser estabelecidas.

Você pode controlar o tipo de LIF no qual uma conexão de dados NDMP é estabelecida usando a `-preferred-interface-role` opção. Durante um estabelecimento de conexão de dados NDMP, o NDMP escolhe um endereço IP que pertence ao tipo LIF, conforme especificado por essa opção. Se os endereços IP não pertencem a nenhum desses tipos de LIF, então a conexão de dados NDMP não pode ser estabelecida. Para obter mais informações sobre a `-preferred-interface-role` opção, consulte as páginas de manual.

Para obter mais informações sobre o `vserver services ndmp modify` comando, consulte as páginas de manual.

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo SVM

O que a extensão Cluster Aware Backup faz

Qual é o modo NDMP com escopo SVM

"Administração do sistema"

Comandos para gerenciar o modo NDMP com escopo SVM

Você pode usar os `vserver services ndmp` comandos para gerenciar NDMP em cada máquina virtual de storage (SVM, anteriormente conhecido como SVM).

Se você quiser…	Use este comando…
Ativar o serviço NDMP	`vserver services ndmp on` O serviço NDMP deve estar sempre habilitado em todos os nós em um cluster. Você pode ativar o serviço NDMP em um nó usando o `system services ndmp on` comando. Por padrão, o serviço NDMP é sempre ativado em um nó.
Desativar o serviço NDMP	`vserver services ndmp off`

Se você quiser…	Use este comando…
Apresentar a configuração NDMP	`vserver services ndmp show`
Modificar a configuração NDMP	`vserver services ndmp modify`
Exibir a versão padrão do NDMP	`vserver services ndmp version`
Exibir todas as sessões NDMP	`vserver services ndmp status`
Exibir informações detalhadas sobre todas as sessões NDMP	`vserver services ndmp probe`
Encerrar uma sessão NDMP especificada	`vserver services ndmp kill`
Encerrar todas as sessões NDMP	`vserver services ndmp kill-all`
Gerar a senha NDMP	`vserver services ndmp generate-password`
Exibir status do ramal NDMP	`vserver services ndmp extensions show` Este comando está disponível no nível de privilégio avançado.
Modificar (ativar ou desativar) o estado da extensão NDMP	`vserver services ndmp extensions modify` Este comando está disponível no nível de privilégio avançado.
Inicie o registo para a sessão NDMP especificada	`vserver services ndmp log start` Este comando está disponível no nível de privilégio avançado.
Parar o registo para a sessão NDMP especificada	`vserver services ndmp log stop` Este comando está disponível no nível de privilégio avançado.

Para obter mais informações sobre esses comandos, consulte as páginas de manual dos `vserver services ndmp` comandos.

O que a extensão Cluster Aware Backup faz

O CAB (Cluster Aware Backup) é uma extensão de protocolo NDMP v4. Essa extensão permite que o servidor NDMP estabeleça uma conexão de dados em um nó que possua um volume. Isso também permite que o aplicativo de backup determine se os volumes e

dispositivos de fita estão localizados no mesmo nó em um cluster.

Para permitir que o servidor NDMP identifique o nó que possui um volume e estabeleça uma conexão de dados em tal nó, o aplicativo de backup deve suportar a EXTENSÃO CAB. A extensão CAB requer que o aplicativo de backup informe o servidor NDMP sobre o volume a ser feito backup ou restaurado antes de estabelecer a conexão de dados. Isso permite que o servidor NDMP determine o nó que hospeda o volume e estabeleça adequadamente a conexão de dados.

Com a EXTENSÃO CAB suportada pelo aplicativo de backup, o servidor NDMP fornece informações de afinidade sobre volumes e dispositivos de fita. Usando essas informações de afinidade, o aplicativo de backup pode executar um backup local em vez de um backup de três vias se um volume e um dispositivo de fita estiverem localizados no mesmo nó em um cluster.

Disponibilidade de volumes e dispositivos de fita para backup e restauração em diferentes tipos de LIF

Você pode configurar um aplicativo de backup para estabelecer uma conexão de controle NDMP em qualquer um dos tipos de LIF em um cluster. No modo NDMP com escopo de máquina virtual de armazenamento (SVM), você pode determinar a disponibilidade de volumes e dispositivos de fita para operações de backup e restauração, dependendo desses tipos de LIF e do status da extensão DA CABINE.

As tabelas a seguir mostram a disponibilidade de volumes e dispositivos de fita para tipos de LIF de conexão de controle NDMP e o status da EXTENSÃO DA CABINE:

Disponibilidade de volumes e dispositivos de fita quando a EXTENSÃO CAB não é suportada pelo aplicativo de backup

Tipo de LIF de conexão de controle NDMP	Volumes disponíveis para backup ou restauração	Dispositivos de fita disponíveis para backup ou restauração
LIF de gerenciamento de nós	Todos os volumes hospedados por um nó	Dispositivos de fita conetados ao nó que hospeda o LIF de gerenciamento de nós
LIF de dados	Somente volumes pertencentes ao SVM hospedados por um nó que hospeda o data LIF	Nenhum
LIF de gerenciamento de clusters	Todos os volumes hospedados por um nó que hospeda o LIF de gerenciamento de cluster	Nenhum
LIF entre clusters	Todos os volumes hospedados por um nó que hospeda o LIF entre clusters	Dispositivos de fita conetados ao nó que hospeda o LIF entre clusters

Disponibilidade de volumes e dispositivos de fita quando a EXTENSÃO CAB é suportada pelo aplicativo de backup

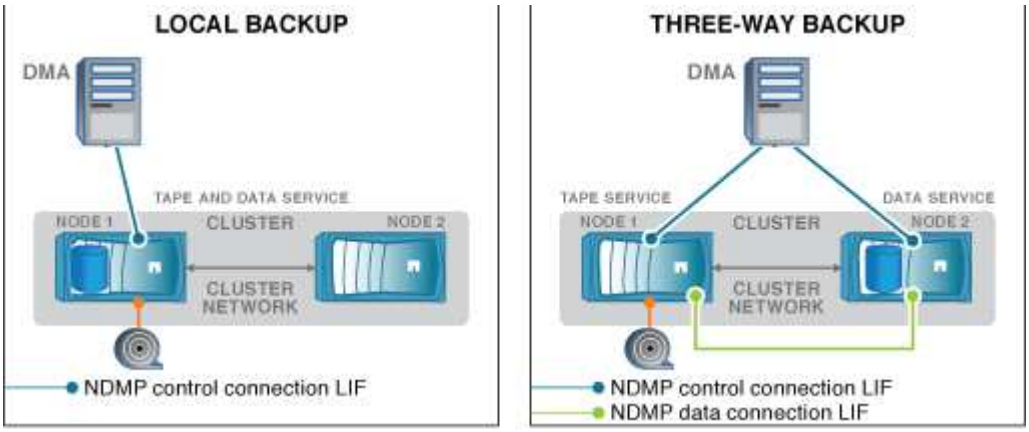
Tipo de LIF de conexão de controle NDMP	Volumes disponíveis para backup ou restauração	Dispositivos de fita disponíveis para backup ou restauração
LIF de gerenciamento de nós	Todos os volumes hospedados por um nó	Dispositivos de fita conetados ao nó que hospeda o LIF de gerenciamento de nós
LIF de dados	Todos os volumes pertencentes ao SVM que hospeda o data LIF	Nenhum
LIF de gerenciamento de clusters	Todos os volumes no cluster	Todos os dispositivos de fita no cluster
LIF entre clusters	Todos os volumes no cluster	Todos os dispositivos de fita no cluster

Que informação de afinidade é

Com o aplicativo de backup ciente DA CAB, o servidor NDMP fornece informações de localização exclusivas sobre volumes e dispositivos de fita. Usando essas informações de afinidade, o aplicativo de backup pode executar um backup local em vez de um backup de três vias se um volume e um dispositivo de fita compartilharem a mesma afinidade.

Se a conexão de controle NDMP for estabelecida em um LIF de gerenciamento de nós, LIF de gerenciamento de cluster ou LIF, o aplicativo de backup poderá usar as informações de afinidade para determinar se um dispositivo de volume e fita está localizado no mesmo nó e, em seguida, executar uma operação de backup ou restauração local ou de três vias. Se a conexão de controle NDMP for estabelecida em um LIF de dados, o aplicativo de backup sempre executará um backup de três vias.

Backup NDMP local e backup NDMP de três vias



Usando as informações de afinidade sobre volumes e dispositivos de fita, o DMA (aplicativo de backup) executa um backup NDMP local no volume e dispositivo de fita localizado no nó 1 no cluster. Se o volume se mover do nó 1 para o nó 2, as informações de afinidade sobre o volume e o dispositivo de fita serão alteradas. Assim, para um backup subsequente, o DMA executa uma operação de backup NDMP de três vias. Isso garante a continuidade da política de backup para o volume, independentemente do nó para o qual o volume é movido.

Informações relacionadas

O que a extensão Cluster Aware Backup faz

O servidor NDMP oferece suporte a conexões de controle seguras no modo com escopo SVM

Uma conexão de controle seguro pode ser estabelecida entre o aplicativo de gerenciamento de dados (DMA) e o servidor NDMP usando soquetes seguros (SSL/TLS) como mecanismo de comunicação. Esta comunicação SSL é baseada nos certificados do servidor. O servidor NDMP escuta na porta 30000 (atribuída pela IANA para o serviço "'ndmps").

Depois de estabelecer a conexão do cliente nesta porta, o handshake SSL padrão segue onde o servidor apresenta o certificado ao cliente. Quando o cliente aceita o certificado, o handshake SSL está concluído. Depois que esse processo estiver concluído, toda a comunicação entre o cliente e o servidor é criptografada. O fluxo de trabalho do protocolo NDMP permanece exatamente como antes. A conexão NDMP segura requer apenas autenticação de certificado do lado do servidor. Um DMA pode optar por estabelecer uma conexão conetando-se ao serviço NDMP seguro ou ao serviço NDMP padrão.

Por padrão, o serviço NDMP seguro é desativado para uma máquina virtual de storage (SVM). Você pode ativar ou desativar o serviço NDMP seguro em um determinado SVM usando o `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` comando.

Tipos de conexão de dados NDMP

No modo NDMP com escopo de máquina virtual de armazenamento (SVM), os tipos de conexão de dados NDMP suportados dependem do tipo de conexão LIF de controle NDMP e do status da extensão DA CABINE. Este tipo de conexão de dados NDMP indica se você pode executar uma operação de backup ou restauração local ou de três vias NDMP.

Você pode executar uma operação de backup ou restauração NDMP de três vias em uma rede TCP ou TCP/IPv6. As tabelas a seguir mostram os tipos de conexão de dados NDMP com base no tipo de LIF de conexão de controle NDMP e no status da EXTENSÃO DA CABINE.

Tipo de conexão de dados NDMP quando a extensão CAB é suportada pelo aplicativo de backup

Tipo de LIF de conexão de controle NDMP	Tipo de conexão de dados NDMP
LIF de gerenciamento de nós	LOCAL, TCP, TCP/IPV6
LIF de dados	TCP, TCP/IPv6
LIF de gerenciamento de clusters	LOCAL, TCP, TCP/IPV6
LIF entre clusters	LOCAL, TCP, TCP/IPV6

Tipo de conexão de dados NDMP quando a EXTENSÃO CAB não é suportada pelo aplicativo de backup

Tipo de LIF de conexão de controle NDMP	Tipo de conexão de dados NDMP
LIF de gerenciamento de nós	LOCAL, TCP, TCP/IPV6
LIF de dados	TCP, TCP/IPv6
LIF de gerenciamento de clusters	TCP, TCP/IPv6
LIF entre clusters	LOCAL, TCP, TCP/IPV6

Informações relacionadas

O que a extensão Cluster Aware Backup faz

"Gerenciamento de rede"

Autenticação de usuário no modo NDMP com escopo SVM

No modo NDMP com escopo de máquina virtual de storage (SVM), a autenticação de usuário NDMP é integrada ao controle de acesso baseado em funções. No contexto SVM, o usuário NDMP deve ter a função "vsadmin" ou "vsadmin-backup". Em um contexto de cluster, o usuário NDMP deve ter a função "'admin'" ou "'backup'".

Além dessas funções pré-definidas, uma conta de usuário associada a uma função personalizada também pode ser usada para autenticação NDMP, desde que a função personalizada tenha a pasta "'vserver services ndmp" em seu diretório de comando e o nível de acesso da pasta não seja "'nenhum'". Nesse modo, você deve gerar uma senha NDMP para uma determinada conta de usuário, que é criada por meio do controle de acesso baseado em função. Os usuários de cluster em uma função de administrador ou backup podem acessar um LIF de gerenciamento de nós, um LIF de gerenciamento de clusters ou um LIF entre clusters. Os usuários em uma função vsadmin-backup ou vsadmin podem acessar apenas o LIF de dados para esse SVM. Portanto, dependendo da função de um usuário, a disponibilidade de volumes e dispositivos de fita para operações de backup e restauração varia.

Este modo também suporta autenticação de utilizador para utilizadores NIS e LDAP. Portanto, os usuários NIS e LDAP podem acessar vários SVMs com um ID de usuário e senha comuns. No entanto, a autenticação NDMP não suporta usuários do ative Directory.

Nesse modo, uma conta de usuário deve estar associada ao aplicativo SSH e ao método de autenticação ""Senha de usuário"".

Informações relacionadas

Comandos para gerenciar o modo NDMP com escopo SVM

"Administração do sistema"

Gerar uma senha específica do NDMP para usuários NDMP

No modo NDMP com escopo de máquina virtual de armazenamento (SVM), você deve gerar uma senha para um ID de usuário específico. A senha gerada é baseada na senha de login real para o usuário NDMP. Se a senha de login real mudar, você deve gerar a senha específica do NDMP novamente.

Passos

1. Use o `vserver services ndmp generate-password` comando para gerar uma senha específica do NDMP.

   Você pode usar essa senha em qualquer operação NDMP atual ou futura que exija a entrada de senha.

   > A partir do contexto de máquina virtual de storage (SVM, anteriormente conhecido como SVM), você pode gerar senhas NDMP para usuários pertencentes apenas a esse SVM.

   O exemplo a seguir mostra como gerar uma senha específica do NDMP para um ID de usuário user1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. Se alterar a palavra-passe para a conta normal do sistema de armazenamento, repita este procedimento para obter a nova palavra-passe específica do NDMP.

Como as operações de backup e restauração em fita são afetadas durante a recuperação de desastres na configuração do MetroCluster

É possível executar operações de backup em fita e restaurar simultaneamente durante a recuperação de desastres em uma configuração do MetroCluster. Você precisa entender como essas operações são afetadas durante a recuperação de desastres.

Se as operações de backup e restauração em fita forem executadas em um volume de SVM em uma relação de recuperação de desastres, você poderá continuar executando backup em fita incremental e restaurar as operações após um switchover e um switchback.

Sobre o motor de descarga para volumes FlexVol

Sobre o motor de descarga para volumes FlexVol

O dump é uma solução de backup e recuperação baseada em cópia Snapshot da ONTAP que ajuda você a fazer backup de arquivos e diretórios de uma cópia Snapshot para um dispositivo de fita e restaurar os dados de backup para um sistema de storage.

Você pode fazer backup dos dados do sistema de arquivos, como diretórios, arquivos e suas configurações de segurança associadas, em um dispositivo de fita usando o backup de despejo. Você pode fazer backup de um volume inteiro, de uma qtree inteiro ou de uma subárvore que não seja um volume inteiro nem uma qtree inteiro.

Você pode executar um backup ou restauração de despejo usando aplicativos de backup compatíveis com NDMP.

Ao executar um backup de despejo, você pode especificar a cópia Snapshot a ser usada para um backup. Se você não especificar uma cópia Snapshot para o backup, o mecanismo de despejo criará uma cópia Snapshot

para o backup. Depois que a operação de backup for concluída, o mecanismo de despejo excluirá essa cópia Snapshot.

Você pode executar backups de nível 0, incrementais ou diferenciais na fita usando o mecanismo de despejo.

> Depois de reverter para uma versão anterior ao Data ONTAP 8.3, você deve executar uma operação de backup de linha de base antes de executar uma operação de backup incremental.

Informações relacionadas

"Atualize, reverta ou downgrade"

Como funciona um backup de despejo

Um backup de despejo grava dados do sistema de arquivos do disco para a fita usando um processo predefinido. Você pode fazer backup de um volume, uma qtree ou uma subárvore que não seja um volume inteiro nem uma qtree inteiro.

A tabela a seguir descreve o processo que o ONTAP usa para fazer backup do objeto indicado pelo caminho de despejo:

Fase	Ação
1	Para backups de volumes inferiores a completos ou de qtree, o ONTAP percorre diretórios para identificar os arquivos a serem copiados. Se você estiver fazendo backup de um volume ou qtree inteiro, o ONTAP combina esse estágio com o Estágio 2.
2	Para um backup de volume completo ou de qtree completo, o ONTAP identifica os diretórios nos volumes ou qtrees a serem copiados.
3	O ONTAP grava os diretórios em fita.
4	O ONTAP grava os arquivos em fita.
5	O ONTAP grava as informações da ACL (se aplicável) na fita.

O backup de despejo usa uma cópia Snapshot de seus dados para o backup. Portanto, você não precisa colocar o volume off-line antes de iniciar o backup.

O backup de despejo nomeia cada cópia Snapshot que ele cria como `snapshot_for_backup.n`, onde `n` é um número inteiro começando em 0. Cada vez que o backup de despejo cria uma cópia Snapshot, ele aumenta o número inteiro em 1. O número inteiro é redefinido para 0 após o sistema de armazenamento ser reiniciado. Depois que a operação de backup for concluída, o mecanismo de despejo excluirá essa cópia Snapshot.

Quando o ONTAP executa vários backups de despejo simultaneamente, o mecanismo de despejo cria várias cópias Snapshot. Por exemplo, se o ONTAP estiver executando dois backups de despejo simultaneamente, você encontrará as seguintes cópias Snapshot nos volumes a partir dos quais os dados estão sendo copiados: `snapshot_for_backup.0` E `snapshot_for_backup.1`.

Quando você está fazendo backup de uma cópia Snapshot, o mecanismo de despejo não cria uma cópia Snapshot adicional.

Tipos de dados que o motor de descarga faz backup

O mecanismo de despejo permite que você faça backup de dados em fita para proteger contra desastres ou interrupções no controlador. Além de fazer backup de objetos de dados, como arquivos, diretórios, qtrees ou volumes inteiros, o mecanismo de despejo pode fazer backup de muitos tipos de informações sobre cada arquivo. Conhecer os tipos de dados que o mecanismo de despejo pode fazer backup e as restrições a serem levadas em consideração podem ajudá-lo a Planejar sua abordagem para a recuperação de desastres.

Além de fazer backup de dados em arquivos, o mecanismo de despejo pode fazer backup das seguintes informações sobre cada arquivo, conforme aplicável:

- UNIX GID, proprietário UID e permissões de arquivo
- Tempo de acesso, criação e modificação do UNIX
- Tipo de ficheiro
- Tamanho do ficheiro
- Nome DOS, atributos dos e tempo de criação
- Listas de controle de acesso (ACLs) com 1.024 entradas de controle de acesso (ACEs)
- Informações de Qtree
- Caminhos de junção

Os caminhos de junção são copiados como links simbólicos.

- Clones de LUN e LUN

  Você pode fazer backup de um objeto LUN inteiro; no entanto, não é possível fazer backup de um único arquivo dentro do objeto LUN. Da mesma forma, você pode restaurar um objeto LUN inteiro, mas não um único arquivo dentro do LUN.

  O mecanismo de despejo faz backup de clones de LUN como LUNs independentes.

- Arquivos alinhados à VM

  O backup de arquivos alinhados à VM não é suportado em versões anteriores ao Data ONTAP 8.1,2.

Quando um clone de LUN com backup de snapshot é transferido do Data ONTAP operando no modo 7 para o ONTAP, ele se torna um LUN inconsistente. O motor de descarga não faz backup de LUNs inconsistentes.

Quando você restaura dados para um volume, a e/S do cliente é restrita nos LUNs sendo restaurados. A restrição LUN é removida apenas quando a operação de restauração de despejo estiver concluída. Da mesma forma, durante uma operação de restauração de um único arquivo ou LUN do SnapMirror, a e/S do cliente é restrita em arquivos e LUNs sendo restaurados. Esta restrição é removida apenas quando a operação de restauração de um único arquivo ou LUN estiver concluída. Se um backup de despejo for executado em um

volume no qual uma restauração de despejo ou uma operação de restauração de arquivo único SnapMirror ou LUN está sendo executada, os arquivos ou LUNs que têm restrição de e/S cliente não serão incluídos no backup. Esses arquivos ou LUNs são incluídos em uma operação de backup subsequente se a restrição de e/S do cliente for removida.

> Um LUN em execução no Data ONTAP 8.3 que é feito backup em fita pode ser restaurado apenas para 8,3 e versões posteriores e não para uma versão anterior. Se o LUN for restaurado para uma versão anterior, o LUN será restaurado como um arquivo.

Quando você faz backup de um volume secundário do SnapVault ou de um destino do volume SnapMirror em fita, apenas os dados do volume são copiados. Não é feito backup dos metadados associados. Portanto, quando você tenta restaurar o volume, apenas os dados nesse volume são restaurados. As informações sobre as relações SnapMirror de volume não estão disponíveis no backup e, portanto, não são restauradas.

Se você despejar um arquivo que tenha apenas permissões do Windows NT e restaurá-lo para uma qtree ou volume de estilo UNIX, o arquivo obtém as permissões UNIX padrão para essa qtree ou volume.

Se você despejar um arquivo que tenha apenas permissões UNIX e restaurá-lo para uma qtree ou volume no estilo NTFS, o arquivo obtém as permissões padrão do Windows para essa qtree ou volume.

Outros despejos e restaurações preservam permissões.

Você pode fazer backup de arquivos alinhados à VM e da `vm-align-sector` opção. Para obter mais informações sobre arquivos alinhados à VM, "Gerenciamento de storage lógico"consulte .

Que cadeias de incremento são

Uma cadeia de incremento é uma série de backups incrementais do mesmo caminho. Como você pode especificar qualquer nível de backup a qualquer momento, você deve entender cadeias de incremento para poder executar backups e restaurações de forma eficaz. Você pode executar 31 níveis de operações de backup incrementais.

Existem dois tipos de cadeias de incremento:

- Uma cadeia de incremento consecutiva, que é uma sequência de backups incrementais que começa com o nível 0 e é aumentada em 1 em cada backup subsequente.
- Uma cadeia de incremento não consecutiva, onde backups incrementais saltam níveis ou têm níveis que estão fora de sequência, como 0, 2, 3, 1, 4 ou mais comumente 0, 1, 2, 1 ou 0, 1, 2, 1, 1.

Os backups incrementais são baseados no backup de nível mais recente. Por exemplo, a sequência dos níveis de backup 0, 2, 3, 1, 4 fornece duas cadeias de incremento: 0, 2, 3 e 0, 1, 4. A tabela a seguir explica as bases dos backups incrementais:

Ordem de cópia de segurança	Nível de incremento	Cadeia de incremento	Base	Cópia de segurança dos ficheiros
1	0	Ambos	Arquivos no sistema de armazenamento	Todos os arquivos no caminho de backup

Ordem de cópia de segurança	Nível de incremento	Cadeia de incremento	Base	Cópia de segurança dos ficheiros
2	2	0, 2, 3	Backup de nível 0	Arquivos no caminho de backup criados desde o backup de nível 0
3	3	0, 2, 3	Backup de nível 2	Arquivos no caminho de backup criados desde o backup de nível 2
4	1	0, 1, 4	Backup de nível 0, porque este é o nível mais recente que é menor do que o backup de nível 1	Arquivos no caminho de backup criados desde o backup de nível 0, incluindo arquivos que estão nos backups de nível 2 e nível 3
5	4	0, 1, 4	O backup de nível 1, por ser um nível mais baixo e mais recente que os backups de nível 0, nível 2 ou nível 3	Arquivos criados desde o backup de nível 1

Qual é o fator de bloqueio

Um bloco de fita é de 1.024 bytes de dados. Durante um backup ou restauração de fita, você pode especificar o número de blocos de fita transferidos em cada operação de leitura/gravação. Esse número é chamado de *fator de bloqueio*.

Você pode usar um fator de bloqueio de 4 a 256. Se você pretende restaurar um backup para um sistema diferente do sistema que fez o backup, o sistema de restauração deve suportar o fator de bloqueio usado para o backup. Por exemplo, se você usar um fator de bloqueio de 128, o sistema no qual você restaura esse backup deve suportar um fator de bloqueio de 128.

Durante um backup NDMP, o MOVER_RECORD_SIZE determina o fator de bloqueio. O ONTAP permite um valor máximo de 256 KB para MOVER_RECORD_size.

Quando reiniciar um backup de despejo

Um backup de despejo às vezes não termina devido a erros internos ou externos, como erros de gravação de fita, interrupções de energia, interrupções acidentais de usuário ou inconsistência interna no sistema de armazenamento. Se o backup falhar por um desses motivos, você poderá reiniciá-lo.

Você pode optar por interromper e reiniciar um backup para evitar períodos de tráfego intenso no sistema de armazenamento ou para evitar a concorrência por outros recursos limitados no sistema de armazenamento, como uma unidade de fita. Você pode interromper um backup longo e reiniciá-lo mais tarde se uma restauração (ou backup) mais urgente exigir a mesma unidade de fita. Os backups reiniciáveis persistem nas reinicializações. Você pode reiniciar um backup abortado para fita somente se as seguintes condições forem verdadeiras:

- A cópia de segurança abortada está na fase IV
- Todas as cópias Snapshot associadas que foram bloqueadas pelo comando dump estão disponíveis.
- O histórico do ficheiro tem de estar ativado.

Quando essa operação de despejo é abortada e deixada em um estado reiniciável, as cópias Snapshot associadas são bloqueadas. Essas cópias Snapshot são liberadas após o contexto de backup ser excluído. Pode visualizar a lista de contextos de cópia de segurança utilizando o `vserver services ndmp restartable backup show` comando.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Como funciona uma restauração de despejo

Uma restauração de despejo grava dados do sistema de arquivos da fita para o disco usando um processo predefinido.

O processo na tabela a seguir mostra como a restauração de despejo funciona:

Fase	Ação
1	O ONTAP cataloga os arquivos que precisam ser extraídos da fita.
2	O ONTAP cria diretórios e arquivos vazios.
3	O ONTAP lê um arquivo da fita, grava-o no disco e define as permissões (incluindo ACLs) nele.
4	O ONTAP repete os estágios 2 e 3 até que todos os arquivos especificados sejam copiados da fita.

Tipos de dados que o motor de descarga restaura

Quando ocorre um desastre ou uma interrupção do controlador, o mecanismo de despejo fornece vários métodos para recuperar todos os dados que você fez backup, de arquivos únicos, para atributos de arquivo, para diretórios inteiros. Conhecer os tipos de dados que o mecanismo de despejo pode restaurar e quando usar qual método de recuperação pode ajudar a minimizar o tempo de inatividade.

Você pode restaurar dados para um LUN on-line mapeado. No entanto, os aplicativos host não podem acessar esse LUN até que a operação de restauração esteja concluída. Após a conclusão da operação de restauração, o cache do host dos dados LUN deve ser lavado para fornecer coerência com os dados restaurados.

O motor de descarga pode recuperar os seguintes dados:

- Conteúdo de arquivos e diretórios
- Permissões de arquivo UNIX
- ACLs

  Se você restaurar um arquivo que tenha apenas permissões de arquivo UNIX para uma qtree ou volume NTFS, o arquivo não tem ACLs do Windows NT. O sistema de armazenamento usa apenas as permissões de arquivo UNIX neste arquivo até que você crie uma ACL do Windows NT nele.

  > Se você restaurar ACLs de backup de sistemas de armazenamento que executam o Data ONTAP 8.2 para sistemas de armazenamento que executam o Data ONTAP 8.1.x e anteriores que tenham um limite ACE inferior a 1.024, uma ACL padrão será restaurada.

- Informações de Qtree

  As informações de Qtree são usadas somente se uma qtree for restaurada para a raiz de um volume. As informações de Qtree não são usadas se uma qtree for restaurada para um diretório inferior, como

`/vs1/vol1/subdir/lowerdir` , e deixar de ser uma qtree.

- Todos os outros atributos de arquivo e diretório
- Fluxos do Windows NT
- LUNs
  - Um LUN deve ser restaurado para um nível de volume ou um nível de qtree para que ele permaneça como um LUN.

    Se for restaurado para um diretório, ele será restaurado como um arquivo porque não contém metadados válidos.

  - Um LUN de 7 modos é restaurado como LUN em um volume ONTAP.
- Um volume do modo 7D pode ser restaurado para um volume ONTAP.
- Os arquivos alinhados à VM restaurados para um volume de destino herdam as propriedades de alinhamento da VM do volume de destino.
- O volume de destino para uma operação de restauração pode ter arquivos com bloqueios obrigatórios ou de aconselhamento.

  Ao executar a operação de restauração para um volume de destino, o motor de descarga ignora esses bloqueios.

Considerações antes de restaurar dados

Você pode restaurar os dados de backup para o caminho original ou para um destino diferente. Se estiver a restaurar dados de cópia de segurança para um destino diferente, tem de preparar o destino para a operação de restauro.

Antes de restaurar dados para o caminho original ou para um destino diferente, você deve ter as seguintes informações e atender aos seguintes requisitos:

- O nível da restauração
- O caminho para o qual você está restaurando os dados
- O fator de bloqueio usado durante o backup
- Se você estiver fazendo uma restauração incremental, todas as fitas devem estar na cadeia de backup
- Uma unidade de fita disponível e compatível com a fita a ser restaurada

Antes de restaurar dados para um destino diferente, você deve executar as seguintes operações:

- Se você estiver restaurando um volume, você deve criar um novo volume.
- Se você estiver restaurando uma qtree ou um diretório, você deve renomear ou mover arquivos que provavelmente tenham os mesmos nomes que os arquivos que você está restaurando.

> No ONTAP 9, os nomes de qtree suportam o formato Unicode. As versões anteriores do ONTAP não suportam este formato. Se uma qtree com nomes Unicode no ONTAP 9 for copiada para uma versão anterior do ONTAP usando o `ndmpcopy` comando ou através da restauração de uma imagem de backup em uma fita, a qtree será restaurada como um diretório regular e não como uma qtree com formato Unicode.

Se um arquivo restaurado tiver o mesmo nome que um arquivo existente, o arquivo existente será substituído pelo arquivo restaurado. No entanto, os diretórios não são sobrescritos.

Para renomear um arquivo, diretório ou qtree durante a restauração sem usar DAR, você deve definir a variável de ambiente EXTRAIR como `E`.

Espaço necessário no sistema de armazenamento de destino

Você precisa de cerca de 100 MB mais espaço no sistema de armazenamento de destino do que a quantidade de dados a serem restaurados.

A operação de restauração verifica a disponibilidade de espaço de volume e inode no volume de destino quando a operação de restauração é iniciada. Definir a variável de ambiente FORÇAR para `Y` fazer com que a operação de restauração pule as verificações de espaço de volume e disponibilidade de inode no caminho de destino. Se não houver espaço de volume suficiente ou inodes disponíveis no volume de destino, a operação de restauração recupera a quantidade de dados permitidos pelo espaço de volume de destino e pela disponibilidade de inodes. A operação de restauração pára quando não há mais espaço de volume ou inodes restantes.

Limites de escalabilidade para sessões de backup e restauração de despejo

Você deve estar ciente do número máximo de sessões de backup e restauração de despejo que podem ser executadas simultaneamente em sistemas de armazenamento de diferentes capacidades de memória do sistema. Este número máximo depende da memória do sistema de um sistema de armazenamento.

Os limites mencionados na tabela a seguir são para o motor de descarga ou restauração. Os limites mencionados nos limites de escalabilidade para sessões NDMP são para o servidor NDMP, que são superiores aos limites do mecanismo.

Memória do sistema de um sistema de armazenamento	Número total de sessões de backup e restauração de despejo
Menos de 16 GB	4
Maior ou igual a 16 GB, mas inferior a 24 GB	16
Maior ou igual a 24 GB	32

Se você usar `ndmpcopy` o comando para copiar dados em sistemas de armazenamento, duas sessões NDMP serão estabelecidas, uma para backup de despejo e outra para restauração de despejo.

Você pode obter a memória do sistema do seu sistema de armazenamento usando o `sysconfig -a` comando (disponível através do nodeshell). Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Informações relacionadas

Limites de escalabilidade para sessões NDMP

Suporte de backup e restauração em fita entre o Data ONTAP operando no modo 7 e o ONTAP

Você pode restaurar dados de backup de um sistema de storage operando no modo 7 ou executando o ONTAP para um sistema de storage operando no modo 7 ou executando o ONTAP.

As seguintes operações de backup e restauração em fita são suportadas entre o Data ONTAP operando no modo 7 e o ONTAP:

- Fazer backup de um volume de 7 modos para uma unidade de fita conetada a um sistema de armazenamento executando o ONTAP
- Fazer backup de um volume ONTAP em uma unidade de fita conetada a um sistema de 7 modos
- Restaurar dados de backup de um volume de 7 modos a partir de uma unidade de fita conetada a um sistema de armazenamento executando o ONTAP
- Restaurar dados de backup de um volume ONTAP de uma unidade de fita conetada a um sistema de modo 7D.
- Restaurar um volume do modo 7D para um volume ONTAP

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Restaurar um volume ONTAP para um volume do modo 7D.

Um LUN ONTAP é restaurado como um arquivo regular em um volume de 7 modos.

Eliminar contextos reiniciáveis

Se você quiser iniciar um backup em vez de reiniciar um contexto, você pode excluir o contexto.

Sobre esta tarefa

Você pode excluir um contexto restartable usando o `vserver services ndmp restartable-backup delete` comando fornecendo o nome SVM e o ID de contexto.

Passos

1. Excluir um contexto restartable:

   `vserver services ndmp restartable-backup delete -vserver *vserver-name* -context -id *context_identifier*`.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Como o dump funciona em um volume secundário do SnapVault

Você pode executar operações de backup em fita em dados espelhados no volume secundário do SnapVault. Você pode fazer backup apenas dos dados espelhados no volume secundário do SnapVault para fita e não dos metadados da relação do SnapVault.

Quando você quebra a relação de espelhamento de proteção de dados (`snapmirror break`) ou quando ocorre uma ressincronização do SnapMirror, sempre é necessário executar um backup de linha de base.

Como o dump funciona com failover de armazenamento e operações ARL

Antes de executar operações de backup ou restauração de despejo, você deve entender como essas operações funcionam com operações de failover de storage (takeover e giveback) ou realocação de agregados (ARL). A `-override-vetoes` opção determina o comportamento do mecanismo de descarga durante uma operação de failover de armazenamento ou ARL.

Quando uma operação de backup ou restauração de despejo está em execução e a `-override-vetoes` opção está definida como `false`, uma operação de failover de armazenamento iniciado pelo usuário ou ARL é interrompida. No entanto, se a `-override-vetoes` opção estiver definida como `true`, a operação de failover de armazenamento ou ARL será continuada e a operação de backup ou restauração de despejo será cancelada. Quando um failover de armazenamento ou operação ARL é iniciado automaticamente pelo sistema de armazenamento, uma operação de backup ou restauração de despejo ativo é sempre abortada. Não é possível reiniciar as operações de backup de despejo e restauração mesmo após a conclusão das

operações de failover de armazenamento ou ARL.

Operações de descarga quando a extensão DA CABINA é suportada

Se o aplicativo de backup suportar a EXTENSÃO CAB, você poderá continuar executando operações de backup e restauração de despejo incremental sem reconfigurar políticas de backup após um failover de armazenamento ou operação ARL.

Operações de descarga quando a extensão DA CABINA não é suportada

Se o aplicativo de backup não suportar a EXTENSÃO CAB, você poderá continuar executando operações de backup e restauração de despejo incremental se você migrar o LIF configurado na política de backup para o nó que hospeda o agregado de destino. Caso contrário, após a operação de failover de armazenamento e ARL, você deve executar um backup de linha de base antes de executar a operação de backup incremental.

Para operações de failover de storage, o LIF configurado na política de backup deve ser migrado para o nó do parceiro.

Informações relacionadas

"Alta disponibilidade"

Como o dump funciona com a movimentação de volume

As operações de backup e restauração em fita e a movimentação de volume podem ser executadas em paralelo até que a fase final de transição seja tentada pelo sistema de storage. Após essa fase, novas operações de backup e restauração de fita não são permitidas no volume que está sendo movido. No entanto, as operações atuais continuam a ser executadas até a conclusão.

A tabela a seguir descreve o comportamento das operações de backup e restauração de fita após a operação de movimentação de volume:

Se você estiver executando operações de backup e restauração de fita na…	Então…
Modo NDMP com escopo de máquina virtual de storage (SVM) quando a EXTENSÃO CAB é suportada pelo aplicativo de backup	Você pode continuar executando operações incrementais de backup em fita e restauração em volumes somente leitura/gravação e leitura sem reconfigurar políticas de backup.
Modo NDMP com escopo SVM quando a EXTENSÃO CAB não é suportada pelo aplicativo de backup	Você pode continuar executando operações incrementais de backup em fita e restauração em volumes somente leitura/gravação e leitura se migrar o LIF configurado na política de backup para o nó que hospeda o agregado de destino. Caso contrário, após a movimentação do volume, você deve executar um backup de linha de base antes de executar a operação de backup incremental.

Quando ocorre uma movimentação de volume, se o volume pertencente a uma SVM diferente no nó de destino tiver o mesmo nome do volume movido, então você não poderá executar operações de backup incrementais do volume movido.

Como o dump funciona quando um FlexVol volume está cheio

Antes de executar uma operação de backup de despejo incremental, você deve garantir que há espaço livre suficiente no FlexVol volume.

Se a operação falhar, você precisará aumentar o espaço livre no volume Flex vol aumentando seu tamanho ou excluindo as cópias Snapshot. Em seguida, execute novamente a operação de backup incremental.

Como o dump funciona quando o tipo de acesso ao volume muda

Quando um volume de destino do SnapMirror ou um volume secundário do SnapVault mudar de estado de leitura/gravação para somente leitura ou de somente leitura para leitura/gravação, você deve executar uma operação de backup ou restauração de fita de linha de base.

O destino do SnapMirror e os volumes secundários do SnapVault são volumes somente leitura. Se você executar operações de backup e restauração em fita nesses volumes, será necessário executar uma operação de backup ou restauração de linha de base sempre que o volume mudar de estado de somente leitura para leitura/gravação ou de leitura/gravação para somente leitura.

Como o dump funciona com um único arquivo SnapMirror ou restauração LUN

Antes de executar operações de backup de despejo ou restauração em um volume para o qual um único arquivo ou LUN é restaurado usando a tecnologia SnapMirror, você deve entender como as operações de despejo funcionam com um único arquivo ou operação de restauração LUN.

Durante uma operação de restauração de um único arquivo ou LUN do SnapMirror, a e/S do cliente é restrita no arquivo ou LUN que está sendo restaurado. Quando a operação de restauração de um único arquivo ou LUN terminar, a restrição de e/S no arquivo ou LUN é removida. Se um backup de despejo for executado em um volume para o qual um único arquivo ou LUN é restaurado, o arquivo ou LUN que tem restrição de e/S cliente não será incluído no backup de despejo. Em uma operação de backup subsequente, esse arquivo ou LUN é feito backup em fita após a restrição de e/S ser removida.

Não é possível executar uma restauração de despejo e uma operação de restauração de arquivo único SnapMirror ou LUN simultaneamente no mesmo volume.

Como as operações de backup e restauração de despejo são afetadas nas configurações do MetroCluster

Antes de executar operações de backup e restauração de despejo em uma configuração do MetroCluster, você deve entender como as operações de despejo são afetadas quando ocorre uma operação de switchover ou switchback.

Operação de backup ou restauração de despejo seguida de switchover

Considere dois clusters: Cluster 1 e cluster 2. Durante uma operação de backup de despejo ou restauração no

cluster 1, se um switchover for iniciado do cluster 1 para o cluster 2, ocorrerá o seguinte:

- Se o valor `override-vetoes` da opção for `false`, o switchover será abortado e a operação de backup ou restauração continua.
- Se o valor da opção for `true`, a operação de backup de despejo ou restauração é abortada e o switchover continua.

Operação de backup ou restauração de despejo seguida de switchback

Um switchover é executado do cluster 1 para o cluster 2 e uma operação de backup ou restauração de despejo é iniciada no cluster 2. A operação de despejo faz backup ou restaura um volume localizado no cluster 2. Neste ponto, se um switchback é iniciado do cluster 2 para o cluster 1, então ocorre o seguinte:

- Se o valor da `override-vetoes` opção for `false`, o switchback é cancelado e a operação de backup ou restauração continua.
- Se o valor da opção for `true`, a operação de backup ou restauração será abortada e o switchback continuará.

Operação de backup ou restauração de despejo iniciada durante um switchover ou switchback

Durante um switchover do cluster 1 para o cluster 2, se uma operação de backup de despejo ou restauração for iniciada no cluster 1, a operação de backup ou restauração falhará e o switchover continuará.

Durante um switchback do cluster 2 para o cluster 1, se uma operação de backup de despejo ou restauração for iniciada do cluster 2, a operação de backup ou restauração falhará e o switchback continuará.

Sobre o motor SMTape para volumes FlexVol

Sobre o motor SMTape para volumes FlexVol

O SMTape é uma solução de recuperação de desastres da ONTAP que faz backup de blocos de dados em fita. Você pode usar o SMTape para realizar backups de volume em fitas. No entanto, você não pode executar um backup no nível de qtree ou subárvore. O SMTape suporta backups de linha de base, diferenciais e incrementais. SMTape não requer uma licença.

Você pode executar uma operação de backup e restauração SMTape usando um aplicativo de backup compatível com NDMP. Você pode escolher SMTape para executar operações de backup e restauração somente no modo NDMP com escopo de máquina virtual de armazenamento (SVM).

> O processo de reversão não é suportado quando uma sessão de backup ou restauração do SMTape está em andamento. Você deve esperar até que a sessão termine ou você deve abortar a sessão NDMP.

Com o SMTape, você pode fazer backup de 255 cópias Snapshot. Para backups subsequentes de linha de base, incrementais ou diferenciais, você precisa excluir cópias Snapshot de backup mais antigas.

Antes de executar uma restauração de linha de base, o volume para o qual os dados estão sendo restaurados deve ser do tipo `DP` e esse volume deve estar no estado restrito. Após uma restauração bem-sucedida, esse volume é automaticamente online. É possível realizar restaurações incrementais ou diferenciais subsequentes nesse volume na ordem em que os backups foram executados.

Use cópias Snapshot durante o backup SMTape

Você deve entender como as cópias Snapshot são usadas durante um backup de linha de base do SMTape e um backup incremental. Há também considerações a ter em mente ao executar um backup usando SMTape.

Backup de linha de base

Durante a execução de um backup de linha de base, você pode especificar o nome da cópia Snapshot a ser feita em backup em fita. Se nenhuma cópia Snapshot for especificada, dependendo do tipo de acesso do volume (leitura/gravação ou somente leitura), uma cópia Snapshot será criada automaticamente ou as cópias Snapshot existentes serão usadas. Quando você especifica uma cópia Snapshot para o backup, todas as cópias Snapshot anteriores à cópia Snapshot especificada também são feitas backup em fita.

Se você não especificar uma cópia Snapshot para o backup, ocorrerá o seguinte:

- Para um volume de leitura/gravação, uma cópia Snapshot é criada automaticamente.

  O backup da cópia Snapshot recém-criada e de todas as cópias Snapshot mais antigas é feito em fita.

- Para um volume somente leitura, o backup de todas as cópias Snapshot, incluindo a cópia Snapshot mais recente, é feito em fita.

  Não é feito o backup de todas as novas cópias Snapshot criadas após o backup ser iniciado.

Backup incremental

Para operações de backup incrementais ou diferenciais do SMTape, os aplicativos de backup compatíveis com NDMP criam e gerenciam as cópias Snapshot.

Você sempre deve especificar uma cópia Snapshot durante a execução de uma operação de backup incremental. Para uma operação de backup incremental bem-sucedida, o backup da cópia Snapshot durante a operação de backup anterior (linha de base ou incremental) deve estar no volume a partir do qual o backup é executado. Para garantir que você use essa cópia Snapshot de backup, considere a política Snapshot atribuída a esse volume enquanto configura a política de backup.

Considerações sobre backups do SMTape em destinos do SnapMirror

- Uma relação de espelho de proteção de dados cria cópias Snapshot temporárias no volume de destino para replicação.

  Você não deve usar essas cópias Snapshot para backup SMTape.

- Se uma atualização do SnapMirror ocorrer em um volume de destino em um relacionamento de espelho de proteção de dados durante uma operação de backup do SMTape no mesmo volume, a cópia Snapshot que é backup do SMTape não deve ser excluída no volume de origem.

  Durante a operação de backup, o SMTape bloqueia a cópia Snapshot no volume de destino e, se a cópia Snapshot correspondente for excluída no volume de origem, a operação de atualização do SnapMirror subsequente falha.

- Você não deve usar essas cópias Snapshot durante o backup incremental.

Capacidades de SMTape

Os recursos do SMTape, como backup de cópias Snapshot, backups incrementais e diferenciais, preservação de recursos de deduplicação e compactação em volumes restaurados e semeadura em fita, ajudam a otimizar suas operações de backup e restauração em fita.

O SMTape oferece os seguintes recursos:

- Fornece uma solução de recuperação de desastres
- Permite backups incrementais e diferenciais
- Faz backup de cópias Snapshot
- Ativa o backup e a restauração de volumes deduplicados e preserva a deduplicação nos volumes restaurados
- Faz backup de volumes compatados e preserva a compactação nos volumes restaurados
- Ativa a semeadura da fita

O SMTape suporta o fator de bloqueio em múltiplos de 4 KB, na faixa de 4 KB a 256 KB.

Você pode restaurar os dados para volumes criados apenas em duas versões consecutivas do ONTAP.

Recursos não suportados no SMTape

O SMTape não suporta backups reiniciáveis e verificação de arquivos de backup.

Limites de escalabilidade para sessões de backup e restauração SMTape

Ao executar operações de backup e restauração SMTape através de NDMP ou CLI (tape seeding), você deve estar ciente do número máximo de sessões de backup e restauração SMTape que podem ser executadas simultaneamente em sistemas de armazenamento com diferentes capacidades de memória do sistema. Este número máximo depende da memória do sistema de um sistema de armazenamento.

Os limites de escalabilidade das sessões de backup e restauração SMTape são diferentes dos limites de sessão NDMP e dos limites de sessão de despejo.

Memória do sistema do sistema de armazenamento	Número total de sessões de backup e restauração SMTape
Menos de 16 GB	6
Maior ou igual a 16 GB, mas inferior a 24 GB	16
Maior ou igual a 24 GB	32

Você pode obter a memória do sistema do seu sistema de armazenamento usando o `sysconfig -a`

comando (disponível através do nodeshell). Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Informações relacionadas

Limites de escalabilidade para sessões NDMP

Limites de escalabilidade para sessões de backup e restauração de despejo

O que é a semeadura da fita

A semeadura de fita é uma funcionalidade SMTape que ajuda você a inicializar um FlexVol volume de destino em uma relação de espelho de proteção de dados.

A semeadura de fita permite estabelecer uma relação de espelho de proteção de dados entre um sistema de origem e um sistema de destino através de uma conexão de baixa largura de banda.

O espelhamento incremental das cópias Snapshot da origem para o destino é viável em uma conexão com baixa largura de banda. No entanto, um espelhamento inicial da cópia Snapshot de base leva muito tempo em uma conexão de baixa largura de banda. Nesses casos, você pode executar um backup SMTape do volume de origem para uma fita e usar a fita para transferir a cópia Snapshot de base inicial para o destino. Em seguida, você pode configurar atualizações incrementais de SnapMirror para o sistema de destino usando a conexão de baixa largura de banda.

Como o SMTape funciona com failover de armazenamento e operações ARL

Antes de executar operações de backup ou restauração do SMTape, você deve entender como essas operações funcionam com operações de failover de armazenamento (aquisição e giveback) ou realocação agregada (ARL). A `-override-vetoes` opção determina o comportamento do mecanismo SMTape durante um failover de armazenamento ou operação ARL.

Quando uma operação de backup ou restauração do SMTape estiver em execução e a `-override-vetoes` opção estiver definida como `false`, um failover de armazenamento iniciado pelo usuário ou operação ARL será interrompido e a operação de backup ou restauração será concluída. Se o aplicativo de backup suportar a EXTENSÃO CAB, você pode continuar executando operações incrementais de backup e restauração de SMTape sem reconfigurar políticas de backup. No entanto, se a `-override-vetoes` opção estiver definida como `true`, a operação de failover de armazenamento ou ARL será continuada e a operação de backup ou restauração SMTape será cancelada.

Informações relacionadas

"Gerenciamento de rede"

"Alta disponibilidade"

Como o SMTape funciona com a movimentação de volume

Operações de backup e operações de movimentação de volume do SMTape podem ser executadas em paralelo até que o sistema de armazenamento tente a fase final de transição. Após essa fase, as novas operações de backup SMTape não podem ser executadas no volume que está sendo movido. No entanto, as operações atuais continuam a ser executadas até a conclusão.

Antes de iniciar a fase de transição para um volume, a operação de movimentação de volume verifica as operações ativas de backup SMTape no mesmo volume. Se houver operações de backup ativas do SMTape, a operação de movimentação de volume passa para um estado de transição diferido e permite que as operações de backup do SMTape sejam concluídas. Depois que essas operações de backup forem concluídas, você deverá reiniciar manualmente a operação de movimentação de volume.

Se o aplicativo de backup suportar a EXTENSÃO CAB, você poderá continuar executando operações incrementais de backup em fita e restauração em volumes somente leitura/gravação e leitura sem reconfigurar políticas de backup.

As operações de restauração de linha de base e movimentação de volume não podem ser executadas simultaneamente; no entanto, a restauração incremental pode ser executada em paralelo com as operações de movimentação de volume, com o comportamento semelhante ao das operações de backup SMTape durante operações de movimentação de volume.

Como o SMTape funciona com operações de rehost de volume

As operações do SMTape não podem começar quando uma operação de rehost de volume está em andamento em um volume. Quando um volume está envolvido em uma operação de rehost de volume, as sessões de SMTape não devem ser iniciadas nesse volume.

Se qualquer operação de rehost de volume estiver em andamento, o backup ou restauração do SMTape falhará. Se um backup ou restauração do SMTape estiver em andamento, as operações de rehost de volume falharão com uma mensagem de erro apropriada. Essa condição se aplica a operações de backup ou restauração baseadas em NDMP e CLI.

Como a política de backup NDMP é afetada durante o ADB

Quando o balanceador de dados automático (ADB) está habilitado, o balanceador analisa as estatísticas de uso de agregados para identificar o agregado que excedeu a porcentagem de uso de alto limite configurada.

Depois de identificar o agregado que excedeu o limite, o balanceador identifica um volume que pode ser movido para agregados residentes em outro nó no cluster e tenta movê-lo. Essa situação afeta a política de backup configurada para esse volume porque se o aplicativo de gerenciamento de dados (DMA) não estiver ciente DA CAB, o usuário terá que reconfigurar a política de backup e executar a operação de backup da linha de base.

> Se o DMA estiver ciente DA CAB e a política de backup tiver sido configurada usando uma interface específica, o ADB não será afetado.

Como as operações de backup e restauração do SMTape são afetadas nas configurações do MetroCluster

Antes de executar operações de backup e restauração do SMTape em uma configuração do MetroCluster, você deve entender como as operações do SMTape são afetadas quando ocorre uma operação de comutação ou switchback.

Operação de backup ou restauração SMTape seguida de switchover

Considere dois clusters: Cluster 1 e cluster 2. Durante uma operação de backup ou restauração do SMTape no cluster 1, se um switchover for iniciado do cluster 1 para o cluster 2, ocorrerá o seguinte:

- Se o valor `-override-vetoes` da opção for `false`, o processo de comutação é abortado e a operação de backup ou restauração continua.
- Se o valor da opção for `true`, a operação de backup ou restauração do SMTape será abortada e o processo de comutação continuará.

Operação de backup ou restauração SMTape seguida de switchback

Um switchover é executado do cluster 1 para o cluster 2 e uma operação de backup ou restauração SMTape é iniciada no cluster 2. A operação SMTape faz backup ou restaura um volume localizado no cluster 2. Neste ponto, se um switchback é iniciado do cluster 2 para o cluster 1, então ocorre o seguinte:

- Se o valor da `-override-vetoes` opção for `false`, o processo de switchback será abortado e a operação de backup ou restauração continuará.
- Se o valor da opção for `true`, a operação de backup ou restauração será abortada e o processo de switchback continuará.

Operação de backup ou restauração SMTape iniciada durante um switchover ou switchback

Durante um processo de comutação do cluster 1 para o cluster 2, se uma operação de backup ou restauração do SMTape for iniciada no cluster 1, a operação de backup ou restauração falhará e o switchover continuará.

Durante um processo de switchback do cluster 2 para o cluster 1, se uma operação de backup ou restauração do SMTape for iniciada a partir do cluster 2, a operação de backup ou restauração falhará e o switchback continuará.

Monitore as operações de backup e restauração em fita para volumes FlexVol

Monitore as operações de backup e restauração em fita para uma visão geral do FlexVol volumes

Você pode exibir os arquivos de log de eventos para monitorar as operações de backup e restauração de fita. O ONTAP Registra automaticamente eventos significativos de backup e restauração e o momento em que eles ocorrem em um arquivo de log chamado `backup` no diretório do controlador `/etc/log/`. Por predefinição, o registo de eventos está definido para `on`.

Talvez você queira exibir arquivos de log de eventos pelos seguintes motivos:

- Verificar se um backup noturno foi bem-sucedido
- Coleta de estatísticas sobre operações de backup
- Para usar as informações em arquivos de log de eventos anteriores para ajudar a diagnosticar problemas com operações de backup e restauração

Uma vez por semana, os arquivos de log de eventos são girados. O `/etc/log/backup` ficheiro é renomeado para `/etc/log/backup.0`, o `/etc/log/backup.0` ficheiro é renomeado para `/etc/log/backup.1`, e assim por diante. O sistema salva os arquivos de log por até seis semanas; portanto, você pode ter até sete arquivos de mensagem (`/etc/log/backup.[0-5]`e o arquivo atual `/etc/log/backup`).

Acesse os arquivos de log de eventos

Você pode acessar os arquivos de log de eventos para operações de backup e restauração de fita `/etc/log/` no diretório usando o `rdfile` comando no nodeshell. Você pode exibir esses arquivos de log de eventos para monitorar operações de backup e restauração de fita.

Sobre esta tarefa

Com configurações adicionais, como uma função de controle de acesso com acesso ao `spi` serviço da Web ou uma conta de usuário configurada com o `http` método de acesso, você também pode usar um navegador da Web para acessar esses arquivos de log.

Passos

1. Para acessar o nodeshell, digite o seguinte comando:

   `node run -node node_name`

   `node_name` é o nome do nó.

2. Para acessar os arquivos de log de eventos para operações de backup e restauração de fita, digite o seguinte comando:

   `rdfile /etc/log/backup`

Informações relacionadas

"Administração do sistema"

O que é o formato de mensagem de log de eventos de despejo e restauração

Descrição geral do formato de mensagem de registo de eventos

Para cada evento de despejo e restauração, uma mensagem é gravada no arquivo de log de backup.

O formato da mensagem de log de eventos de despejo e restauração é o seguinte:

`type timestamp identifier event (event_info)`

A lista a seguir descreve os campos no formato de mensagem de log de eventos:

- Cada mensagem de log começa com um dos indicadores de tipo descritos na tabela a seguir:

Tipo	Descrição
registo	A registar evento
dmp	Evento de despejo
rst	Restaurar evento

- `timestamp` mostra a data e a hora do evento.
- O `identifier` campo para um evento de despejo inclui o caminho de despejo e o ID exclusivo para o despejo. O `identifier` campo para um evento de restauração usa apenas o nome do caminho de destino de restauração como um identificador exclusivo. As mensagens de eventos relacionadas ao log não incluem um `identifier` campo.

Quais são os eventos de Registro

O campo evento de uma mensagem que começa com um log especifica o início de um log ou o fim de um log.

Ele contém um dos eventos mostrados na tabela a seguir:

Evento	Descrição
Start_Logging (Iniciar registo)	Indica o início do registo ou que o registo foi ligado novamente após ser desativado.
Stop_Logging (Parar registo)	Indica que o registo foi desativado.

Quais são os eventos de despejo

O campo evento para um evento de despejo contém um tipo de evento seguido de informações específicas do evento entre parênteses.

A tabela a seguir descreve os eventos, suas descrições e as informações de eventos relacionados que podem ser gravadas para uma operação de despejo:

Evento	Descrição	Informações sobre eventos
Iniciar	O despejo NDMP é iniciado	Nível de despejo e o tipo de despejo
Fim	Despejos concluídos com sucesso	Quantidade de dados processados
Abortar	A operação é cancelada	Quantidade de dados processados
Opções	As opções especificadas são listadas	Todas as opções e seus valores associados, incluindo opções NDMP
Tape_open (fita aberta)	A fita está aberta para leitura/gravação	O novo nome do dispositivo de fita
Tape_Close (Fechar fita)	A fita está fechada para leitura/gravação	O nome do dispositivo de fita

Evento	Descrição	Informações sobre eventos
Mudança de fase	Um despejo está entrando em uma nova fase de processamento	O nome da nova fase
Erro	Um despejo encontrou um evento inesperado	Mensagem de erro
Snapshot	Uma cópia Snapshot é criada ou localizada	O nome e a hora da cópia Snapshot
Base_dump	Foi localizada uma entrada de despejo base no metafile interno	O nível e o tempo do despejo base (apenas para despejos incrementais)

Quais são os eventos de restauração

O campo evento para um evento de restauração contém um tipo de evento seguido de informações específicas de eventos entre parênteses.

A tabela a seguir fornece informações sobre os eventos, suas descrições e as informações de eventos relacionados que podem ser gravadas para uma operação de restauração:

Evento	Descrição	Informações sobre eventos
Iniciar	A restauração NDMP é iniciada	Nível de restauração e tipo de restauração
Fim	Restaurações concluídas com êxito	Número de arquivos e quantidade de dados processados
Abortar	A operação é cancelada	Número de arquivos e quantidade de dados processados
Opções	As opções especificadas são listadas	Todas as opções e seus valores associados, incluindo opções NDMP
Tape_open (fita aberta)	A fita está aberta para leitura/gravação	O novo nome do dispositivo de fita
Tape_Close (Fechar fita)	A fita está fechada para leitura/gravação	O nome do dispositivo de fita
Mudança de fase	Restaurar está entrando em uma nova fase de processamento	O nome da nova fase

Evento	Descrição	Informações sobre eventos
Erro	Restaurar encontros com um evento inesperado	Mensagem de erro

Ativar ou desativar o registo de eventos

Pode ativar ou desativar o registo de eventos.

Passos

1. Para ativar ou desativar o log de eventos, digite o seguinte comando no clustershell:

   `options -option_name backup.log.enable -option-value {on | off}`

   `on` ativa o registo de eventos.

   `off` desativa o registo de eventos.

   O registo de eventos está ativado por predefinição.

Mensagens de erro para backup em fita e restauração de volumes FlexVol

Fazer backup e restaurar mensagens de erro

Limitação de recursos: nenhum tópico disponível

- **Mensagem**

  `Resource limitation: no available thread`

- **Causa**

  O número máximo de threads de e/S de fita locais ativos está atualmente em uso. Você pode ter um máximo de 16 unidades de fita locais ativas.

- **Ações corretivas**

  Aguarde que alguns trabalhos de fita sejam concluídos antes de iniciar um novo trabalho de backup ou restauração.

Reserva de fita preemptada

- **Mensagem**

  `Tape reservation preempted`

- **Causa**

  A unidade de fita está em uso por outra operação ou a fita foi fechada prematuramente.

- **Ações corretivas**

Certifique-se de que a unidade de fita não está em uso por outra operação e que o aplicativo DMA não cancelou o trabalho e tente novamente.

Não foi possível inicializar o suporte

- **Mensagem**

  `Could not initialize media`

- **Causa**

  Você pode receber esse erro por um dos seguintes motivos:

  - A unidade de fita usada para o backup está corrompida ou danificada.
  - A fita não contém o backup completo ou está corrompida.
  - O número máximo de threads de e/S de fita locais ativos está atualmente em uso.

    Você pode ter um máximo de 16 unidades de fita locais ativas.

- **Ações corretivas**
  - Se a unidade de fita estiver corrompida ou danificada, tente novamente a operação com uma unidade de fita válida.
  - Se a fita não contiver o backup completo ou estiver corrompida, não será possível executar a operação de restauração.
  - Se os recursos de fita não estiverem disponíveis, aguarde que alguns dos trabalhos de backup ou restauração sejam concluídos e tente novamente a operação.

Número máximo de despejos ou restaurações permitidos (limite máximo de sessão) em andamento

- **Mensagem**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Causa**

  O número máximo de trabalhos de cópia de segurança ou restauro já está em execução.

- **Ações corretivas**

  Tente novamente a operação depois que alguns dos trabalhos atualmente em execução tiverem sido concluídos.

Erro de Mídia na gravação da fita

- **Mensagem**

  `Media error on tape write`

- **Causa**

  A fita usada para o backup está corrompida.

- **Ações corretivas**

  Substitua a fita e tente novamente o trabalho de backup.

Falha na gravação em fita

- **Mensagem**

  ```
  Tape write failed
  ```

- **Causa**

  A fita usada para o backup está corrompida.

- **Ações corretivas**

  Substitua a fita e tente novamente o trabalho de backup.

Falha na gravação da fita - erro de Mídia encontrado na nova fita

- **Mensagem**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Causa**

  A fita usada para o backup está corrompida.

- **Ações corretivas**

  Substitua a fita e tente novamente o backup.

Falha na gravação da fita - a nova fita está quebrada ou protegida contra gravação

- **Mensagem**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Causa**

  A fita usada para o backup está corrompida ou protegida contra gravação.

- **Ações corretivas**

  Substitua a fita e tente novamente o backup.

Falha na gravação em fita - a nova fita já está no final do material

- **Mensagem**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Causa**

Não há espaço suficiente na fita para concluir o backup.

- **Ações corretivas**

  Substitua a fita e tente novamente o backup.

Erro de gravação da fita

- **Mensagem**

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- **Causa**

  A capacidade da fita é insuficiente para conter os dados de backup.

- **Ações corretivas**

  Use fitas com maior capacidade e tente novamente o trabalho de backup.

Erro de Mídia na leitura da fita

- **Mensagem**

  ```
  Media error on tape read
  ```

- **Causa**

  A fita a partir da qual os dados estão sendo restaurados está corrompida e pode não conter os dados completos de backup.

- **Ações corretivas**

  Se tiver certeza de que a fita tem o backup completo, tente novamente a operação de restauração. Se a fita não contiver o backup completo, não será possível executar a operação de restauração.

Erro de leitura da fita

- **Mensagem**

  ```
  Tape read error
  ```

- **Causa**

  A unidade de fita está danificada ou a fita não contém o backup completo.

- **Ações corretivas**

  Se a unidade de fita estiver danificada, use outra unidade de fita. Se a fita não contiver o backup completo, não será possível restaurar os dados.

Já no final da fita

- **Mensagem**

  ```
  Already at the end of tape
  ```

- **Causa**

  A fita não contém dados nem deve ser enrolada novamente.

- **Ações corretivas**

  Se a fita não contiver dados, use a fita que contém o backup e tente novamente o trabalho de restauração. Caso contrário, rebobine a fita e tente novamente o trabalho de restauração.

O tamanho do Registro da fita é muito pequeno. Tente um tamanho maior.

- **Mensagem**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Causa**

  O fator de bloqueio especificado para a operação de restauração é menor do que o fator de bloqueio usado durante o backup.

- **Ações corretivas**

  Use o mesmo fator de bloqueio especificado durante o backup.

O tamanho do Registro da fita deve ser block_size1 e não block_size2

- **Mensagem**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Causa**

  O fator de bloqueio especificado para a restauração local está incorreto.

- **Ações corretivas**

  Tente novamente o trabalho de restauração com `block_size1` o como fator de bloqueio.

O tamanho do Registro da fita deve estar no intervalo entre 4KB e 256KB

- **Mensagem**

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- **Causa**

  O fator de bloqueio especificado para a operação de backup ou restauração não está dentro do intervalo permitido.

- **Ações corretivas**

  Especifique um fator de bloqueio no intervalo de 4 KB a 256 KB.

Mensagens de erro NDMP

Erro de comunicação de rede

- **Mensagem**

  ```
  Network communication error
  ```

- **Causa**

  A comunicação com uma fita remota em uma conexão de três vias NDMP falhou.

- **Ações corretivas**

  Verifique a ligação de rede ao motor remoto.

Mensagem do soquete de leitura: Error_string

- **Mensagem**

  ```
  Message from Read Socket: error_string
  ```

- **Causa**

  Restaurar a comunicação da fita remota na conexão NDMP de 3 vias tem erros.

- **Ações corretivas**

  Verifique a ligação de rede ao motor remoto.

Mensagem de Write Dirnet: Error_string

- **Mensagem**

  ```
  Message from Write Dirnet: error_string
  ```

- **Causa**

  A comunicação de backup para uma fita remota em uma conexão de três vias NDMP tem um erro.

- **Ações corretivas**

  Verifique a ligação de rede ao motor remoto.

Tomada de leitura recebida EOF

- **Mensagem**

  ```
  Read Socket received EOF
  ```

- **Causa**

  A tentativa de se comunicar com uma fita remota em uma conexão de três vias NDMP chegou ao fim da marca File. Você pode estar tentando uma restauração de três vias a partir de uma imagem de backup com um tamanho de bloco maior.

- **Ações corretivas**

  Especifique o tamanho correto do bloco e tente novamente a operação de restauração.

ndmpd número de versão inválido: version_number "

- **Mensagem**

  `ndmpd invalid version number: version_number`

- **Causa**

  A versão NDMP especificada não é suportada pelo sistema de storage.

- **Ações corretivas**

  Especifique a versão 4 do NDMP.

Sessão ndmpd session_ID não ativa

- **Mensagem**

  `ndmpd session session_ID not active`

- **Causa**

  A sessão NDMP pode não existir.

- **Ações corretivas**

  Use o `ndmpd status` comando para exibir as sessões NDMP ativas.

Não foi possível obter vol Ref para volume volume_name

- **Mensagem**

  `Could not obtain vol ref for Volume vol_name`

- **Causa**

  Não foi possível obter a referência de volume porque o volume pode estar a ser utilizado por outras operações.

- **Ações corretivas**

  Tente novamente a operação mais tarde.

Tipo de conexão de dados ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] não suportado para conexões de controle ["IPv6"|"IPv4"]

- **Mensagem**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- **Causa**

  No modo NDMP com escopo de nó, a conexão de dados NDMP estabelecida deve ser do mesmo tipo de endereço de rede (IPv4 ou IPv6) que a conexão de controle NDMP.

- **Ações corretivas**

  Entre em Contato com o fornecedor do aplicativo de backup.

ESCUTA DE DADOS: Conexão de dados DA CABINE preparar erro de pré-condição

- **Mensagem**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Causa**

  A escuta de dados NDMP falha quando o aplicativo de backup negociou a extensão CAB com o servidor NDMP e há uma incompatibilidade no tipo de endereço de conexão de dados NDMP especificado entre as mensagens NDMP_CAB_DATA_CONN_PREPARE e NDMP_DATA_LISTEN.

- **Ações corretivas**

  Entre em Contato com o fornecedor do aplicativo de backup.

CONEXÃO DE DADOS: Conexão de dados DA CAB preparar erro de pré-condição

- **Mensagem**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Causa**

  A conexão de dados NDMP falha quando o aplicativo de backup negociou a extensão CAB com o servidor NDMP e há uma incompatibilidade no tipo de endereço de conexão de dados NDMP especificado entre as mensagens NDMP_CAB_DATA_CONN_PREPARE e NDMP_DATA_CONNECT.

- **Ações corretivas**

  Entre em Contato com o fornecedor do aplicativo de backup.

Erro:show failed: Não é possível obter a senha do usuário '<username>'

- **Mensagem**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Causa**

  Configuração incompleta da conta de usuário para NDMP

- **Ações corretivas**

  Certifique-se de que a conta de utilizador está associada ao método de acesso SSH e que o método de autenticação é a palavra-passe de utilizador.

Mensagens de erro de despejo

O volume de destino é somente leitura

- **Mensagem**

  ```
  Destination volume is read-only
  ```

- **Causa**

  O caminho para o qual a operação de restauração é tentada é somente leitura.

- **Ações corretivas**

  Tente restaurar os dados para um local diferente.

A qtree de destino é somente leitura

- **Mensagem**

  ```
  Destination qtree is read-only
  ```

- **Causa**

  A qtree para a qual a restauração é tentada é somente leitura.

- **Ações corretivas**

  Tente restaurar os dados para um local diferente.

Despejos temporariamente desativados no volume, tente novamente

- **Mensagem**

  ```
  Dumps temporarily disabled on volume, try again
  ```

- **Causa**

  Tentativa de backup de despejo NDMP em um volume de destino do SnapMirror que faz parte de `snapmirror break` uma operação ou de uma `snapmirror resync`.

- **Ações corretivas**

  Aguarde até que a `snapmirror break` operação ou `snapmirror resync` termine e, em seguida, efetue a operação de descarga.

Sempre que o estado de um volume de destino do SnapMirror mudar de leitura/gravação para somente leitura ou de somente leitura para leitura/gravação, você deve executar um backup de linha de base.

Rótulos NFS não reconhecidos

- **Mensagem**

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- **Causa**

  As etiquetas de segurança NFS são suportadas a partir do ONTAP 9.9,1 quando o NFSv4,2 está ativado. No entanto, as etiquetas de segurança NFS não são reconhecidas atualmente pelo mecanismo de despejo. Se ele encontrar quaisquer rótulos de segurança NFS nos arquivos, diretórios ou quaisquer arquivos especiais em qualquer formato de despejo, o despejo falhará.

- **Ações corretivas**

  Verifique se nenhum arquivo ou diretório tem rótulos de segurança NFS.

Não foram criados ficheiros

- **Mensagem**

  ```
  No files were created
  ```

- **Causa**

  Um DAR de diretório foi tentado sem habilitar a funcionalidade DAR aprimorada.

- **Ações corretivas**

  Ative a funcionalidade DAR melhorada e tente novamente DAR.

A restauração do arquivo <file name> falhou

- **Mensagem**

  ```
  Restore of the file file name failed
  ```

- **Causa**

  Quando um DAR (Direct Access Recovery) de um arquivo cujo nome de arquivo é o mesmo que o de um LUN no volume de destino é executado, o DAR falha.

- **Ações corretivas**

  Tente DAR novamente do arquivo.

Falha no truncamento para src inode <inode number>…

- **Mensagem**

  `Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.`

- **Causa**

  Inode de um arquivo é excluído quando o arquivo está sendo restaurado.

- **Ações corretivas**

  Aguarde até que a operação de restauração em um volume seja concluída antes de usar esse volume.

Não é possível bloquear um instantâneo necessário pelo despejo

- **Mensagem**

  `Unable to lock a snapshot needed by dump`

- **Causa**

  A cópia Snapshot especificada para o backup não está disponível.

- **Ações corretivas**

  Tente novamente o backup com uma cópia Snapshot diferente.

  Use o `snap list` comando para ver a lista de cópias Snapshot disponíveis.

Não foi possível localizar ficheiros bitmap

- **Mensagem**

  `Unable to locate bitmap files`

- **Causa**

  Os arquivos bitmap necessários para a operação de backup podem ter sido excluídos. Neste caso, o backup não pode ser reiniciado.

- **Ações corretivas**

  Efetue a cópia de segurança novamente.

O volume está temporariamente em um estado de transição

- **Mensagem**

  `Volume is temporarily in a transitional state`

- **Causa**

O volume que está a ser guardado está temporariamente num estado não montado.

- **Ações corretivas**

  Aguarde algum tempo e efetue a cópia de segurança novamente.

Mensagens de erro SMTape

Pedaços fora de ordem

- **Mensagem**

  ```
  Chunks out of order
  ```

- **Causa**

  As fitas de backup não estão sendo restauradas na sequência correta.

- **Ações corretivas**

  Repita a operação de restauração e carregue as fitas na sequência correta.

Formato de bloco não suportado

- **Mensagem**

  ```
  Chunk format not supported
  ```

- **Causa**

  A imagem de backup não é do SMTape.

- **Ações corretivas**

  Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha o backup do SMTape.

Falha ao alocar memória

- **Mensagem**

  ```
  Failed to allocate memory
  ```

- **Causa**

  O sistema ficou sem memória.

- **Ações corretivas**

  Tente novamente o trabalho mais tarde quando o sistema não estiver muito ocupado.

Falha ao obter buffer de dados

- **Mensagem**

  ```
  Failed to get data buffer
  ```

- **Causa**

  O sistema de armazenamento ficou sem buffers.

- **Ações corretivas**

  Aguarde até que algumas operações do sistema de armazenamento sejam concluídas e, em seguida, tente novamente o trabalho.

Falha ao encontrar instantâneo

- **Mensagem**

  ```
  Failed to find snapshot
  ```

- **Causa**

  A cópia Snapshot especificada para o backup não está disponível.

- **Ações corretivas**

  Verifique se a cópia Snapshot especificada está disponível. Caso contrário, tente novamente com a cópia Snapshot correta.

Falha ao criar instantâneo

- **Mensagem**

  ```
  Failed to create snapshot
  ```

- **Causa**

  O volume já contém o número máximo de cópias Snapshot.

- **Ações corretivas**

  Exclua algumas cópias Snapshot e tente novamente a operação de backup.

Falha ao bloquear instantâneo

- **Mensagem**

  ```
  Failed to lock snapshot
  ```

- **Causa**

  A cópia Snapshot está em uso ou foi excluída.

- **Ações corretivas**

  Se a cópia Snapshot estiver a ser utilizada por outra operação, aguarde que a operação termine e, em seguida, tente novamente a cópia de segurança. Se a cópia Snapshot tiver sido excluída, não será possível executar a cópia de segurança.

Falha ao eliminar instantâneo

- **Mensagem**

  `Failed to delete snapshot`

- **Causa**

  A cópia Snapshot automática não pôde ser excluída porque está em uso por outras operações.

- **Ações corretivas**

  Use o `snap` comando para determinar o status da cópia Snapshot. Se a cópia Snapshot não for necessária, exclua-a manualmente.

Falha ao obter instantâneo mais recente

- **Mensagem**

  `Failed to get latest snapshot`

- **Causa**

  A cópia Snapshot mais recente pode não existir porque o volume está sendo inicializado pelo SnapMirror.

- **Ações corretivas**

  Tente novamente após a inicialização estar concluída.

Falha ao carregar nova fita

- **Mensagem**

  `Failed to load new tape`

- **Causa**

  Erro na unidade de fita ou Mídia.

- **Ações corretivas**

  Substitua a fita e tente novamente a operação.

Falha ao inicializar a fita

- **Mensagem**

```
Failed to initialize tape
```

- **Causa**

  Você pode receber esta mensagem de erro por um dos seguintes motivos:

  - A imagem de backup não é do SMTape.
  - O fator de bloqueio da fita especificado está incorreto.
  - A fita está corrompida ou danificada.
  - A fita errada é carregada para restauração.

- **Ações corretivas**
  - Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha backup do SMTape.
  - Se o fator de bloqueio estiver incorreto, especifique o fator de bloqueio correto e tente novamente a operação.
  - Se a fita estiver corrompida, não será possível executar a operação de restauração.
  - Se a fita errada estiver carregada, tente novamente a operação com a fita correta.

Falha ao inicializar o fluxo de restauração

- **Mensagem**

```
Failed to initialize restore stream
```

- **Causa**

  Você pode receber esta mensagem de erro por um dos seguintes motivos:

  - A imagem de backup não é do SMTape.
  - O fator de bloqueio da fita especificado está incorreto.
  - A fita está corrompida ou danificada.
  - A fita errada é carregada para restauração.

- **Ações corretivas**
  - Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha o backup do SMTape.
  - Se o fator de bloqueio estiver incorreto, especifique o fator de bloqueio correto e tente novamente a operação.
  - Se a fita estiver corrompida, não será possível executar a operação de restauração.
  - Se a fita errada estiver carregada, tente novamente a operação com a fita correta.

Falha ao ler a imagem de cópia de segurança

- **Mensagem**

```
Failed to read backup image
```

- **Causa**

A fita está corrompida.

- **Ações corretivas**

  Se a fita estiver corrompida, não será possível executar a operação de restauração.

Cabeçalho da imagem ausente ou corrompido

- **Mensagem**

  ```
  Image header missing or corrupted
  ```

- **Causa**

  A fita não contém um backup SMTape válido.

- **Ações corretivas**

  Tente novamente com uma fita contendo um backup válido.

Asserção interna

- **Mensagem**

  ```
  Internal assertion
  ```

- **Causa**

  Existe um erro interno do SMTape.

- **Ações corretivas**

  Comunique o erro e envie o `etc/log/backup` ficheiro para o suporte técnico.

Número mágico da imagem de cópia de segurança inválido

- **Mensagem**

  ```
  Invalid backup image magic number
  ```

- **Causa**

  A imagem de backup não é do SMTape.

- **Ações corretivas**

  Se a imagem de backup não for do SMTape, tente novamente a operação com uma fita que tenha o backup do SMTape.

Soma de verificação da imagem de cópia de segurança inválida

- **Mensagem**

```
Invalid backup image checksum
```

- **Causa**

  A fita está corrompida.

- **Ações corretivas**

  Se a fita estiver corrompida, não será possível executar a operação de restauração.

Fita de entrada inválida

- **Mensagem**

  ```
  Invalid input tape
  ```

- **Causa**

  A assinatura da imagem de backup não é válida no cabeçalho da fita. A fita possui dados corrompidos ou não contém uma imagem de backup válida.

- **Ações corretivas**

  Tente novamente o trabalho de restauro com uma imagem de cópia de segurança válida.

Caminho de volume inválido

- **Mensagem**

  ```
  Invalid volume path
  ```

- **Causa**

  O volume especificado para a operação de backup ou restauração não foi encontrado.

- **Ações corretivas**

  Tente novamente o trabalho com um caminho de volume e um nome de volume válidos.

Incompatibilidade na ID do conjunto de cópias de segurança

- **Mensagem**

  ```
  Mismatch in backup set ID
  ```

- **Causa**

  A fita carregada durante uma mudança de fita não faz parte do conjunto de backup.

- **Ações corretivas**

  Carregue a fita correta e tente novamente o trabalho.

Não correspondência no carimbo de hora de cópia de segurança

- **Mensagem**

  ```
  Mismatch in backup time stamp
  ```

- **Causa**

  A fita carregada durante uma mudança de fita não faz parte do conjunto de backup.

- **Ações corretivas**

  Use o `smtape restore -h` comando para verificar as informações do cabeçalho de uma fita.

Trabalho cancelado devido ao encerramento

- **Mensagem**

  ```
  Job aborted due to shutdown
  ```

- **Causa**

  O sistema de armazenamento está sendo reinicializado.

- **Ações corretivas**

  Tente novamente o trabalho depois que o sistema de armazenamento for reiniciado.

Trabalho cancelado devido a snapshot autodelete

- **Mensagem**

  ```
  Job aborted due to Snapshot autodelete
  ```

- **Causa**

  O volume não tem espaço suficiente e acionou a exclusão automática de cópias Snapshot.

- **Ações corretivas**

  Liberte espaço no volume e tente novamente o trabalho.

A fita está atualmente em uso por outras operações

- **Mensagem**

  ```
  Tape is currently in use by other operations
  ```

- **Causa**

  A unidade de fita está em uso por outro trabalho.

- **Ações corretivas**

Tente novamente a cópia de segurança após o trabalho atualmente ativo terminar.

Fitas fora de ordem

- **Mensagem**

  ```
  Tapes out of order
  ```

- **Causa**

  A primeira fita da sequência da fita para a operação de restauração não tem o cabeçalho da imagem.

- **Ações corretivas**

  Carregue a fita com o cabeçalho da imagem e tente novamente o trabalho.

Falha na transferência (cancelada devido à operação MetroCluster)

- **Mensagem**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Causa**

  A operação SMTape é abortada devido a uma operação de comutação ou comutação.

- **Ações corretivas**

  Execute a operação SMTape após o término da operação de comutação ou switchback.

Falha na transferência (interrupção iniciada ARL)

- **Mensagem**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Causa**

  Enquanto uma operação SMTape estiver em andamento se uma realocação agregada for iniciada, a operação SMTape será abortada.

- **Ações corretivas**

  Execute a operação SMTape após a conclusão da operação de realocação de agregados.

Falha na transferência (interrupção iniciada pelo CFO)

- **Mensagem**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Causa**

  A operação SMTape é abortada devido a uma operação de failover de armazenamento (aquisição e

giveback) de um agregado CFO.

- **Ações corretivas**

  Executar a operação SMTape após o failover de armazenamento do CFO agregado terminar.

Falha na transferência (cancelamento iniciado pelo SFO)

- **Mensagem**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Causa**

  A operação SMTape é abortada devido a uma operação de failover de armazenamento (aquisição e giveback).

- **Ações corretivas**

  Execute a operação SMTape após a conclusão da operação de failover de armazenamento (aquisição e giveback).

Agregado subjacente sob migração

- **Mensagem**

  ```
  Underlying aggregate under migration
  ```

- **Causa**

  Se uma operação SMTape for iniciada em um agregado que está sob migração (failover de armazenamento ou realocação agregada), a operação SMTape falhará.

- **Ações corretivas**

  Execute a operação SMTape depois que a migração agregada terminar.

O volume está atualmente em migração

- **Mensagem**

  ```
  Volume is currently under migration
  ```

- **Causa**

  A migração de volume e o backup SMTape não podem ser executados simultaneamente.

- **Ações corretivas**

  Tente novamente o trabalho de cópia de segurança após a conclusão da migração de volume.

Volume off-line

- **Mensagem**

  `Volume offline`

- **Causa**

  O volume que está sendo feito backup está offline.

- **Ações corretivas**

  Coloque o volume on-line e tente novamente o backup.

Volume não restrito

- **Mensagem**

  `Volume not restricted`

- **Causa**

  O volume de destino para o qual os dados estão sendo restaurados não é restrito.

- **Ações corretivas**

  Restrinja o volume e tente novamente a operação de restauração.

Configuração NDMP

Visão geral da configuração NDMP

Você pode configurar rapidamente um cluster ONTAP 9 para usar o Protocolo de gerenciamento de dados de rede (NDMP) para fazer backup de dados diretamente em fita usando um aplicativo de backup de terceiros.

Se o aplicativo de backup oferecer suporte ao Cluster Aware Backup (CAB), você poderá configurar o NDMP como *SVM-scoped* ou *node-scoped*:

- O escopo do SVM no nível do cluster (admin SVM) permite fazer backup de todos os volumes hospedados em diferentes nós do cluster. NDMP com escopo SVM é recomendado, sempre que possível.
- O NDMP com escopo de nó permite fazer backup de todos os volumes hospedados nesse nó.

Se o aplicativo de backup não suportar CAB, você deve usar NDMP com escopo de nó.

NDMP com escopo SVM e escopo de nó são mutuamente exclusivos; eles não podem ser configurados no mesmo cluster.

O NDMP com escopo de nó está obsoleto no ONTAP 9.

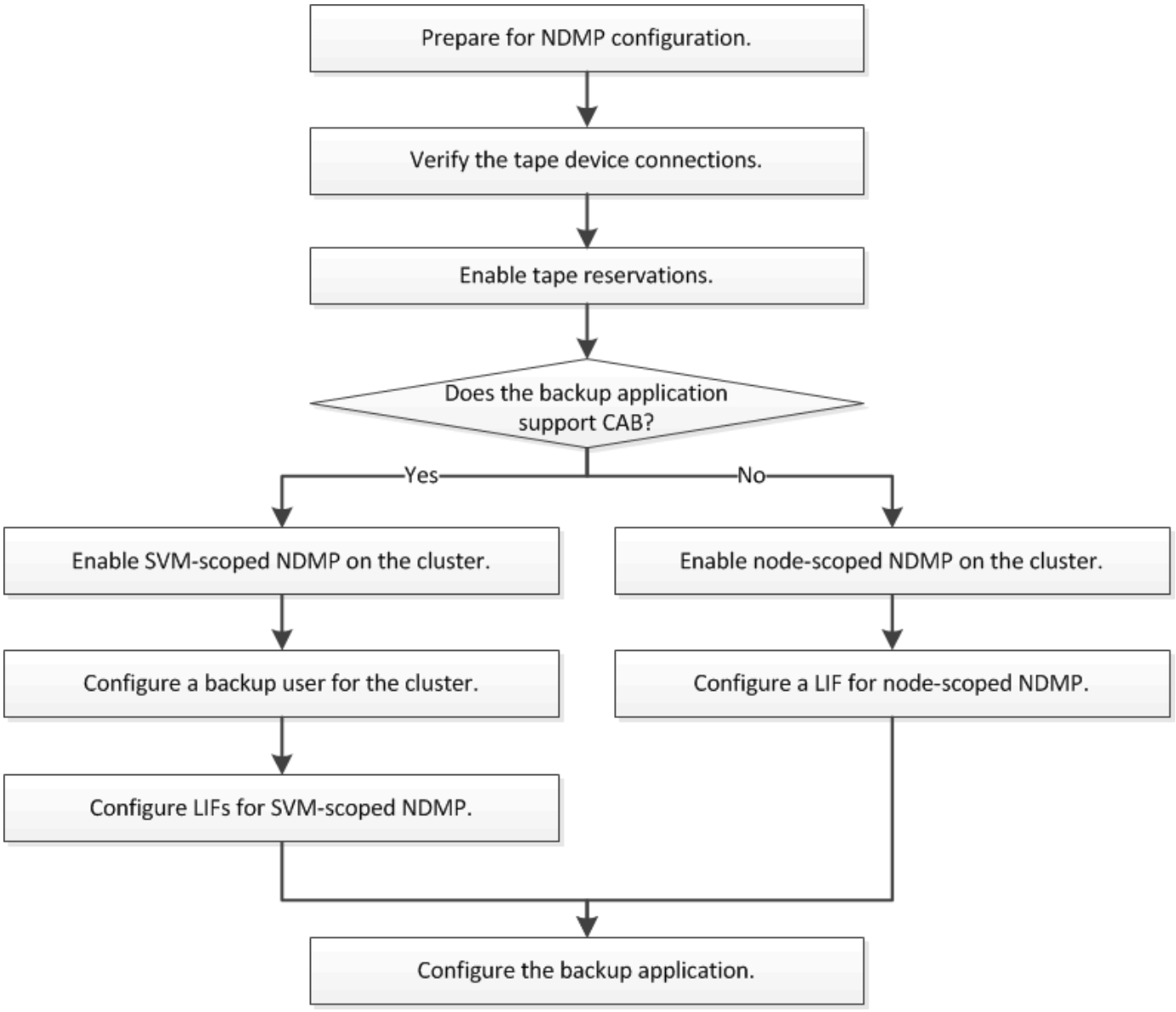
Saiba mais "Backup ciente de cluster (CAB)"sobre o .

Antes de configurar o NDMP, verifique o seguinte:

- Você tem um aplicativo de backup de terceiros (também chamado de aplicativo de gerenciamento de dados ou DMA).
- Você é um administrador de cluster.
- Dispositivos de fita e um servidor de Mídia opcional estão instalados.
- Os dispositivos de fita são conetados ao cluster por meio de um switch Fibre Channel (FC) ou conetados localmente.
- Pelo menos um dispositivo de fita tem um número de unidade lógica (LUN) de 0.

Fluxo de trabalho de configuração NDMP

A configuração do backup em fita no NDMP envolve a preparação para a configuração NDMP, a verificação das conexões do dispositivo de fita, a ativação de reservas de fita, a configuração do NDMP no nível do SVM ou nó, a ativação do NDMP no cluster, a configuração de um usuário de backup, a configuração de LIFs e a configuração do aplicativo de backup.



Prepare-se para a configuração NDMP

Antes de configurar o acesso de backup em fita pelo Network Data Management Protocol (NDMP), você deve verificar se a configuração planejada é suportada, verificar se suas unidades de fita estão listadas como unidades qualificadas em cada nó, verificar se todos os nós têm LIFs entre clusters e identificar se o aplicativo de backup suporta a extensão CAB (Cluster Aware Backup).

Passos

1. Consulte a matriz de compatibilidade do fornecedor do aplicativo de backup para obter suporte ao ONTAP (o NetApp não qualifica aplicativos de backup de terceiros com ONTAP ou NDMP).

   Você deve verificar se os seguintes componentes do NetApp são compatíveis:

   - A versão do ONTAP 9 que está sendo executada no cluster.
   - O fornecedor e a versão do aplicativo de backup: Por exemplo, Veritas NetBackup 8,2 ou CommVault.

- Os detalhes dos dispositivos de fita, como o fabricante, o modelo e a interface das unidades de fita: Por exemplo, IBM Ultrium 8 ou HPE StoreEver Ultrium 30750 LTO-8.
- As plataformas dos nós no cluster: Por exemplo, FAS8700 ou A400.

> Você pode encontrar matrizes de suporte de compatibilidade legadas do ONTAP para aplicativos de backup no "Ferramenta de Matriz de interoperabilidade do NetApp".

2. Verifique se suas unidades de fita estão listadas como unidades qualificadas no arquivo de configuração de fita interno de cada nó:

   a. Na interface de linha de comando, visualize o arquivo de configuração de fita incorporado usando o `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                 Is
Tape Drives                      Supported  Support Status
-------------------------------  ---------
--------------------------------
Certance Ultrium 2               true       Dynamically Qualified
Certance Ultrium 3               true       Dynamically Qualified
Digital DLT2000                  true       Qualified
```

   b. Compare suas unidades de fita com a lista de unidades qualificadas na saída.

> Os nomes dos dispositivos de fita na saída podem variar ligeiramente dos nomes na etiqueta do dispositivo ou na Matriz de interoperabilidade. Por exemplo, o Digital DLT2000 também pode ser conhecido como DLT2k. Você pode ignorar essas pequenas diferenças de nomenclatura.

   c. Se um dispositivo não estiver listado como qualificado na saída, mesmo que o dispositivo esteja qualificado de acordo com a Matriz de interoperabilidade, baixe e instale um arquivo de configuração atualizado para o dispositivo usando as instruções no site de suporte da NetApp.

      "Downloads do NetApp: Arquivos de configuração do dispositivo de fita"

   Um dispositivo qualificado pode não estar listado no arquivo de configuração de fita incorporado se o dispositivo de fita tiver sido qualificado após o nó ser enviado.

3. Verifique se cada nó no cluster tem um LIF entre clusters:

   a. Visualize as LIFs entre clusters nos nós usando o `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

b. Se um LIF entre clusters não existir em nenhum nó, crie um LIF entre clusters usando o `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

"Gerenciamento de rede"

4. Identifique se o aplicativo de backup suporta Backup ciente de cluster (CAB) usando a documentação fornecida com o aplicativo de backup.

   O suporte DA CAB é um fator chave para determinar o tipo de backup que você pode executar.

Verifique as conexões do dispositivo de fita

Você deve garantir que todas as unidades e alteradores de Mídia estejam visíveis no ONTAP como dispositivos.

Passos

1. Veja informações sobre todas as unidades e modificadores de Mídia usando o `storage tape show` comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID               Device Type     Description
Status
----------------------  -------------  ------------------------------
--------
sw4:10.11               tape drive      HP LTO-3
normal
0b.125L1                media changer   HP MSL G3 Series
normal
0d.4                    tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                  media changer   IBM 3573-TL
normal
...
```

2. Se uma unidade de fita não for exibida, solucione o problema.
3. Se um trocador de Mídia não for exibido, exiba informações sobre alteradores de Mídia usando o `storage tape show-media-changer` comando e solucione o problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Ative as reservas de fita

Você deve garantir que as unidades de fita sejam reservadas para uso por aplicativos de backup para operações de backup NDMP.

Sobre esta tarefa

As configurações de reserva variam em diferentes aplicativos de backup, e essas configurações devem corresponder ao aplicativo de backup e aos nós ou servidores que usam as mesmas unidades. Consulte a documentação do fornecedor do aplicativo de backup para obter as configurações corretas de reserva.

Passos

1. Ative as reservas usando o `options -option-name tape.reservations -option-value persistent` comando.

   O seguinte comando permite reservas com o `persistent` valor:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Verifique se as reservas estão ativadas em todos os nós usando o `options tape.reservations` comando e, em seguida, revise a saída.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                persistent

   cluster1-2
       tape.reservations                persistent
   2 entries were displayed.
   ```

Configurar NDMP com escopo SVM

Habilite NDMP com escopo SVM no cluster

Se o DMA oferecer suporte à extensão CAB (Cluster Aware Backup), você poderá fazer backup de todos os volumes hospedados em diferentes nós em um cluster habilitando NDMP com escopo SVM, habilitando o serviço NDMP no cluster (admin SVM) e configurando LIFs para conexão de dados e controle.

O que você vai precisar

A extensão DA CABINA tem de ser suportada pelo DMA.

Sobre esta tarefa

Desativar o modo NDMP com escopo de nó ativa o modo NDMP com escopo SVM no cluster.

Passos

1. Ativar o modo NDMP com escopo SVM:

```
cluster1::> system services ndmp node-scope-mode off
```

O modo NDMP com escopo SVM está ativado.

2. Habilite o serviço NDMP no administrador SVM:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

O tipo de autenticação é definido como `challenge` por padrão e a autenticação de texto sem formatação é desativada.

> Para uma comunicação segura, você deve manter a autenticação em texto simples desativada.

3. Verifique se o serviço NDMP está ativado:

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Ative um usuário de backup para autenticação NDMP

Para autenticar NDMP com escopo SVM a partir do aplicativo de backup, deve haver um usuário administrativo com Privileges suficiente e uma senha NDMP.

Sobre esta tarefa

Você deve gerar uma senha NDMP para usuários de administração de backup. É possível habilitar usuários de administração de backup no nível de cluster ou SVM e, se necessário, criar um novo usuário. Por padrão, os usuários com as seguintes funções podem se autenticar para backup NDMP:

- Em todo o cluster: `admin` Ou `backup`
- SVMs individuais: `vsadmin` Ou `vsadmin-backup`

Se estiver a utilizar um utilizador NIS ou LDAP, o utilizador tem de existir no respetivo servidor. Você não pode usar um usuário do ative Directory.

Passos

1. Exibir os usuários e permissões de administrador atuais:

```
security login show
```

2. Se necessário, crie um novo usuário de backup NDMP com o `security login create` comando e a função apropriada para o SVM Privileges individual ou em todo o cluster.

   Pode especificar um nome de utilizador de cópia de segurança local ou um nome de utilizador NIS ou LDAP para o `-user-or-group-name` parâmetro.

   O comando a seguir cria o usuário de backup `backup_admin1` com a `backup` função para todo o cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   O comando a seguir cria o usuário de `vsbackup_admin1` backup com a `vsadmin-backup` função de um SVM individual:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Introduza uma palavra-passe para o novo utilizador e confirme.

3. Gere uma senha para o administrador SVM usando o `vserver services ndmp generate password` comando.

   A senha gerada deve ser usada para autenticar a conexão NDMP pelo aplicativo de backup.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   Password: qG5CqQHYxw7tE57g
   ```

Configurar LIFs

Você precisa identificar os LIFs que serão usados para estabelecer uma conexão de dados entre os recursos de dados e fita, e para conexão de controle entre o SVM admin e o aplicativo de backup. Depois de identificar os LIFs, você deve verificar se as políticas de serviço e failover estão definidas.

A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Gerencie o tráfego suportado"consulte .

ONTAP 9.10,1 ou posterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Identifique o LIF de gerenciamento hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

   ```
   network interface show -service-policy default-management
   ```

3. Certifique-se de que o LIF entre clusters inclui o `backup-ndmp-control` serviço:

   ```
   network interface service-policy show
   ```

4. Certifique-se de que a política de failover esteja definida adequadamente para todos os LIFs:

   a. Verifique se a política de failover para o gerenciamento de cluster está definida como `broadcast-domain-wide`, e se a política para LIFs de gerenciamento de clusters e nós está definida como `local-only` usando o `network interface show -failover` comando.

      O comando a seguir exibe a política de failover para as LIFs de gerenciamento de clusters, clusters e nós:

```
cluster1::> network interface show -failover

          Logical          Home             Failover    Failover
Vserver   Interface        Node:Port        Policy      Group
-------   --------------   --------------   ----------  --------
cluster   cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                        Failover
Targets:
                                                        .......
cluster1  cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                        Failover
Targets:
                                                        .......
          IC1              cluster1-1:e0a   local-only  Default
                                                        Failover
Targets:
          IC2              cluster1-1:e0b   local-only  Default
                                                        Failover
Targets:
                                                        .......
cluster1-1 c1-1_mgmt1      cluster1-1:e0m   local-only  Default
                                                        Failover
Targets:
                                                        ......
cluster1-2 c1-2_mgmt1      cluster1-2:e0m   local-only  Default
                                                        Failover
Targets:
                                                        ......
```

a. Se as políticas de failover não forem definidas adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

5. Especifique os LIFs necessários para a conexão de dados usando o `vserver services ndmp modify` comando com o `preferred-interface-role` parâmetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Verifique se a função de interface preferida está definida para o cluster usando o `vserver`

`services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9 1.9 ou anterior

Passos

1. Identifique os LIFs entre clusters, gerenciamento de cluster e gerenciamento de nós usando o `network interface show` comando com o `-role` parâmetro.

   O comando a seguir exibe as LIFs entre clusters:

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   O comando a seguir exibe o LIF de gerenciamento de cluster:

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

   O comando a seguir exibe as LIFs de gerenciamento de nó:

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

2. Certifique-se de que a política de firewall está ativada para NDMP nos (`node-mgmt`LIFs entre clusters, gerenciamento de cluster (`cluster-mgmt`) e gerenciamento de nós):

   a. Verifique se a política de firewall está habilitada para NDMP usando o `system services firewall policy show` comando.

      O comando a seguir exibe a política de firewall para o LIF de gerenciamento de cluster:

      ```
      cluster1::> system services firewall policy show -policy cluster

      Vserver     Policy       Service    Allowed
      -------     ------------ ---------- -----------------
      cluster     cluster      dns        0.0.0.0/0
                               http       0.0.0.0/0
                               https      0.0.0.0/0
                               ndmp       0.0.0.0/0
                               ndmps      0.0.0.0/0
                               ntp        0.0.0.0/0
                               rsh        0.0.0.0/0
                               snmp       0.0.0.0/0
                               ssh        0.0.0.0/0
                               telnet     0.0.0.0/0
      10 entries were displayed.
      ```

      O comando a seguir exibe a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

O comando a seguir exibe a política de firewall para o LIF de gerenciamento de nós:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Se a política de firewall não estiver ativada, ative a política de firewall utilizando o `system services firewall policy modify` comando com o `-service` parâmetro.

O seguinte comando ativa a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Certifique-se de que a política de failover esteja definida adequadamente para todos os LIFs:

a. Verifique se a política de failover para o gerenciamento de cluster está definida como `broadcast-domain-wide`, e se a política para LIFs de gerenciamento de clusters e nós está definida como `local-only` usando o `network interface show -failover` comando.

   O comando a seguir exibe a política de failover para as LIFs de gerenciamento de clusters, clusters e nós:

```
cluster1::> network interface show -failover

          Logical            Home               Failover
Failover
Vserver   Interface          Node:Port          Policy
Group
--------- -----------------  ----------------- --------------------
--------
cluster   cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                    Failover
Targets:
                                                    .......

cluster1  cluster_mgmt       cluster1-1:e0m    broadcast-domain-
wide Default
                                                    Failover
Targets:
                                                    .......
          IC1                 cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
          IC2                 cluster1-1:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1 cluster1-1_mgmt1  cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    ......
cluster1-2 cluster1-2_mgmt1  cluster1-2:e0m    local-only
Default
                                                    Failover
Targets:
                                                    ......
```

a. Se as políticas de failover não forem definidas adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Especifique os LIFs necessários para a conexão de dados usando o `vserver services ndmp modify` comando com o `preferred-interface-role` parâmetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verifique se a função de interface preferida está definida para o cluster usando o `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

Configurar NDMP com escopo de nó

Habilite NDMP com escopo de nó no cluster

Você pode fazer backup de volumes hospedados em um único nó habilitando NDMP com escopo de nó, habilitando o serviço NDMP e configurando um LIF para conexão de dados e controle. Isso pode ser feito para todos os nós do cluster.

O NDMP com escopo de nó está obsoleto no ONTAP 9.

Sobre esta tarefa

Ao usar NDMP no modo de escopo de nó, a autenticação deve ser configurada por nó. Para obter mais informações, "O artigo da base de dados de Conhecimento "como configurar a autenticação NDMP no modo 'nó-escopo'""consulte .

Passos

1. Ativar o modo NDMP com escopo de nó:

```
cluster1::> system services ndmp node-scope-mode on
```

O modo de escopo do nó NDMP está ativado.

2. Habilite o serviço NDMP em todos os nós do cluster:

   O uso do curinga "'*" permite o serviço NDMP em todos os nós ao mesmo tempo.

   Você deve especificar uma senha para autenticação da conexão NDMP pelo aplicativo de backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Desative a `-clear-text` opção de comunicação segura da senha NDMP:

   Usando a opção curinga "'*" `disables the `-clear-text` em todos os nós ao mesmo tempo.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Verifique se o serviço NDMP está ativado e se a `-clear-text` opção está desativada:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configurar um LIF

Você deve identificar um LIF que será usado para estabelecer uma conexão de dados e controlar a conexão entre o nó e o aplicativo de backup. Depois de identificar o LIF, você deve verificar se as políticas de firewall e failover estão definidas para o LIF.

> A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Gerencie o tráfego suportado"consulte .

ONTAP 9.10,1 ou posterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-service-policy` parâmetro.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Certifique-se de que o LIF entre clusters inclui o `backup-ndmp-control` serviço:

   ```
   network interface service-policy show
   ```

3. Certifique-se de que a política de failover esteja definida adequadamente para os LIFs entre clusters:

   a. Verifique se a política de failover para os LIFs entre clusters está definida como `local-only` usando o `network interface show -failover` comando.

   ```
   cluster1::> network interface show -failover
               Logical          Home               Failover
   Failover
   Vserver     Interface        Node:Port          Policy       Group
   --------    ---------------  -----------------  ------------
   --------
   cluster1    IC1               cluster1-1:e0a    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
               IC2               cluster1-2:e0b    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   ```

   b. Se a política de failover não for definida adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

   ```
   cluster1::> network interface modify -vserver cluster1 -lif IC1
   -failover-policy local-only
   ```

ONTAP 9 1.9 ou anterior

Passos

1. Identifique o LIF entre clusters hospedado nos nós usando o `network interface show` comando com o `-role` parâmetro.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. Certifique-se de que a política de firewall está ativada para NDMP nos LIFs entre clusters:

   a. Verifique se a política de firewall está habilitada para NDMP usando o `system services firewall policy show` comando.

   O comando a seguir exibe a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. Se a política de firewall não estiver ativada, ative a política de firewall utilizando o `system services firewall policy modify` comando com o `-service` parâmetro.

   O seguinte comando ativa a política de firewall para o LIF entre clusters:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Certifique-se de que a política de failover esteja definida adequadamente para os LIFs entre clusters:
   a. Verifique se a política de failover para os LIFs entre clusters está definida como `local-only` usando o `network interface show -failover` comando.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. Se a política de failover não for definida adequadamente, modifique a política de failover usando o `network interface modify` comando com o `-failover-policy` parâmetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configure a aplicação de cópia de segurança

Depois que o cluster é configurado para o acesso NDMP, você deve coletar informações da configuração do cluster e, em seguida, configurar o resto do processo de backup no aplicativo de backup.

Passos

1. Reúna as seguintes informações que você configurou anteriormente no ONTAP:
   - O nome de usuário e a senha que o aplicativo de backup requer para criar a conexão NDMP
   - Os endereços IP das LIFs entre clusters que o aplicativo de backup requer para se conetar ao cluster
2. No ONTAP, exiba os aliases atribuídos pelo ONTAP a cada dispositivo usando o `storage tape alias show` comando.

   Os aliases são muitas vezes úteis na configuração do aplicativo de backup.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                          Alias     Mapping
----------------------------- --------- ------------------------------
stsw-3220-4a-4b-02            st2       SN[HU19497WVR]
...
```

3. No aplicativo de backup, configure o restante do processo de backup usando a documentação do aplicativo de backup.

Depois de terminar

Se ocorrer um evento de mobilidade de dados, como uma movimentação de volume ou migração de LIF, você deve estar preparado para reinicializar quaisquer operações de backup interrompidas.

Visão geral da replicação entre o software NetApp Element e o ONTAP

Você pode garantir a continuidade dos negócios em um sistema Element usando o SnapMirror para replicar cópias Snapshot de um volume Element para um destino ONTAP. No caso de um desastre no local do Element, você pode fornecer dados aos clientes a partir do sistema ONTAP e reativar o sistema Element quando o serviço for restaurado.

A partir do ONTAP 9.4, é possível replicar cópias Snapshot de um LUN criado em um nó ONTAP de volta para um sistema Element. Você pode ter criado um LUN durante uma interrupção no site do Element ou pode estar usando um LUN para migrar dados do software ONTAP para o Element.

"Configurar a replicação do software NetApp Element e do ONTAP".

Monitoramento de eventos, desempenho e integridade

Monitore o desempenho do cluster com o System Manager

Monitore o desempenho do cluster usando o System Manager

Os tópicos nesta seção mostram como gerenciar a integridade e o desempenho do cluster com o System Manager no ONTAP 9.7 e versões posteriores.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para monitorar o desempenho do cluster. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Você pode monitorar o desempenho do cluster exibindo informações sobre o sistema no Painel do System Manager. O Dashboard exibe informações sobre alertas e notificações importantes, a eficiência e a capacidade das camadas e volumes de storage, os nós disponíveis em um cluster, o status dos nós em um par de HA, as aplicações e objetos mais ativos e as métricas de performance de um cluster ou nó.

O Dashboard permite determinar as seguintes informações:

- **Saúde**: Quão saudável é o cluster?
- **Capacidade**: Que capacidade está disponível no cluster?
- **Desempenho**: O desempenho do cluster com base na latência, IOPS e taxa de transferência?
- **Rede**: Como a rede é configurada com hosts e objetos de armazenamento, como portas, interfaces e VMs de armazenamento?

Nas visões gerais de integridade e capacidade, você pode clicar → para exibir informações adicionais e executar tarefas.

Na Visão geral de desempenho, você pode visualizar as métricas com base na hora, no dia, na semana, no mês ou no ano.

Na visão geral da rede, o número de cada objeto na rede é exibido (por exemplo, "8 portas NVMe/FC"). Você pode clicar nos números para exibir detalhes sobre cada objeto de rede.

Veja a visão geral do cluster no painel do System Manager

O dashboard do System Manager oferece uma visualização rápida e abrangente do cluster do ONTAP em um único local.

Com o dashboard do System Manager, você pode visualizar informações gerais sobre alertas e notificações importantes, a eficiência e a capacidade das camadas e volumes de storage, os nós disponíveis em um cluster, o status dos nós em um par de alta disponibilidade (HA), as aplicações e objetos mais ativos e as métricas de performance de um cluster ou nó.

O painel de instrumentos inclui quatro painéis descritos da seguinte forma:

Saúde

O modo de exibição integridade exibe informações sobre a integridade geral de todos os nós detetáveis no cluster.

A visualização Saúde também exibe os erros e avisos no nível do cluster, como detalhes do nó não configurados, indicando as caraterísticas que podem ser modificadas para melhorar o desempenho do cluster.

Clique → para expandir a visualização Saúde para obter uma visão geral do cluster, como o nome do cluster, a versão, a data e hora de criação do cluster e muito mais. Você também pode monitorar as estatísticas relacionadas à integridade dos nós associados a um cluster. Você pode gerenciar tags que permitem agrupar e identificar recursos em seu ambiente. A seção Insights ajuda a otimizar a capacidade, a conformidade de segurança e a configuração do seu sistema.

Capacidade

A exibição capacidade exibe o espaço de armazenamento de um cluster. Você pode visualizar o espaço lógico total usado, o espaço físico total usado e o espaço em disco disponível.

Você pode optar por se Registrar no ActiveIQ para visualizar os dados históricos do cluster. Clique → para expandir a visualização capacidade para ver uma visão geral dos níveis associados a um cluster. É possível exibir informações de capacidade sobre cada uma das camadas: O espaço total, o espaço usado e o espaço disponível. Os detalhes são exibidos para taxa de transferência, IOPS e latência. "Saiba mais sobre essas medições de capacidade no System Manager".

Você pode optar por adicionar uma categoria local ou uma categoria de nuvem usando a visualização de capacidade. Para obter mais informações sobre a exibição capacidade, "Exibir a capacidade de um cluster"consulte .

Rede

O modo de exibição rede exibe as portas físicas, as interfaces de rede e as VMs de armazenamento que fazem parte da rede.

O modo de exibição rede exibe o tipo de clientes conetados à rede. Cada um desses clientes conectados à rede é representado por um número (por exemplo, "NVMe/FC 16"). Selecione o número para visualizar detalhes específicos em cada um desses elementos de rede.

Clique → para ver uma visualização expansiva de página inteira da rede que engloba portas, interfaces de rede, VMs de armazenamento e hosts na rede.

Desempenho

A visualização desempenho exibe estatísticas de desempenho para ajudar a monitorar a integridade e a eficiência do cluster do ONTAP. As estatísticas incluem os principais indicadores de desempenho do cluster, como latência, taxa de transferência e IOPS, representados como gráficos.

A visualização desempenho apresenta estatísticas de desempenho em diferentes intervalos de tempo por dia, hora, semana ou ano. Você pode analisar rapidamente o desempenho do cluster usando os vários gráficos e identificar as caraterísticas que podem exigir otimização. Essa análise rápida ajuda você a decidir como adicionar ou mover cargas de trabalho. Você também pode olhar para os horários de pico de uso para Planejar possíveis mudanças.

A visualização de performance exibe as métricas totais de performance relacionadas à latência, taxa de transferência e IOPS.

A partir de 9.15.1, a visualização de desempenho é aprimorada para exibir gráficos para métricas de desempenho de leitura, gravação, outras e totais relacionadas à latência, taxa de transferência e IOPS. Outras métricas incluem quaisquer operações que não sejam lidas ou gravadas.

Os valores de performance são atualizados a cada 3 segundos e o gráfico de performance é atualizado a cada 15 segundos. Um gráfico não será exibido se as informações sobre o desempenho do cluster não estiverem disponíveis.

Clique para ver uma visualização de página inteira das métricas de desempenho por hora, dia, semana, mês e ano. Você também pode baixar um relatório das métricas de desempenho em seu sistema local.

Identificar volumes ativos e outros objetos

Acelere a performance do cluster identificando os volumes (hot volumes) e dados acessados com frequência (hot objetos).

A partir do ONTAP 9.10,1, você pode usar o recurso Rastreamento de atividades no sistema de arquivos Analytics para monitorar objetos ativos em um volume.

Passos

1. Clique em **armazenamento > volumes**.
2. Filtre as colunas IOPS, latência e taxa de transferência para visualizar os volumes e dados acessados com frequência.

Modificar QoS

A partir do ONTAP 9.8, quando você provisiona o storage, Qualidade do serviço (QoS) é habilitado por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento. Também é possível modificar a QoS depois que o storage tiver sido provisionado.

Passos

1. No System Manager, selecione **Storage** e depois **volumes**.
2. Ao lado do volume para o qual você deseja modificar QoS, selecione **Editar**.

Monitorar riscos

A partir do ONTAP 9.10,0, você pode usar o Gerenciador do sistema para monitorar os riscos relatados pelo consultor digital da Active IQ (também conhecido como consultor digital). A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para reconhecer os riscos.

O consultor digital da NetApp relata oportunidades para reduzir riscos e melhorar a performance e a eficiência do seu ambiente de storage. Com o System Manager, você pode aprender sobre os riscos relatados pelo Digital Advisor e receber inteligência acionável que ajuda a administrar o storage e a obter maior disponibilidade, maior segurança e melhor desempenho de storage.

Link para sua conta do Digital Advisor

Para receber informações sobre riscos do Digital Advisor, primeiro você deve vincular a sua conta do Digital Advisor do System Manager.

Passos

1. No System Manager, clique em **Cluster > Settings**.
2. Em **Registo Active IQ**, clique em **Registo**.
3. Introduza as suas credenciais para o Digital Advisor.
4. Depois que suas credenciais forem autenticadas, clique em **Confirm (confirmar) para vincular o Active IQ ao Gerenciador do sistema**.

Veja o número de riscos

A partir do ONTAP 9.10,0, você pode visualizar no painel do Gerenciador de sistemas o número de riscos relatados pelo Consultor Digital.

Antes de começar

Você deve estabelecer uma conexão do System Manager com sua conta do Digital Advisor. Link para sua conta do Digital AdvisorConsulte a .

Passos

1. No System Manager, clique em **Dashboard**.
2. Na seção **Saúde**, veja o número de riscos relatados.

> Você pode ver informações mais detalhadas sobre cada risco clicando na mensagem mostrando o número de riscos. Ver detalhes dos riscosConsulte .

Ver detalhes dos riscos

A partir do ONTAP 9.10,0, você pode ver no Gerenciador de sistemas como os riscos relatados pelo Consultor Digital são categorizados por áreas de impactos. Você também pode exibir informações detalhadas sobre cada risco relatado, seu potencial impactos no seu sistema e ações corretivas que você pode tomar.

Antes de começar

Você deve estabelecer uma conexão do System Manager com sua conta do Digital Advisor. Link para sua conta do Digital AdvisorConsulte a .

Passos

1. Clique em **Eventos > todos os eventos**.
2. Na seção **Visão geral**, em **sugestões de Active IQ**, veja o número de riscos em cada categoria de área de impactos. As categorias de risco incluem:
   - Desempenho e eficiência
   - Disponibilidade e proteção
   - Capacidade
   - Configuração
   - Segurança

3. Clique na guia **sugestões de Active IQ** para visualizar informações sobre cada risco, incluindo o seguinte:
    - Nível de impactos no seu sistema
    - Categoria do risco
    - Nós afetados
    - Tipo de mitigação necessária
    - Ações corretivas que você pode tomar

Reconheça os riscos

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para reconhecer qualquer um dos riscos abertos.

Passos

1. No System Manager, exiba a lista de riscos executando o procedimento Ver detalhes dos riscosem .
2. Clique no nome de risco de um risco aberto que você deseja reconhecer.
3. Insira as informações nos seguintes campos:
    - Lembrete (data)
    - Justificação
    - Comentários
4. Clique em **confirmar**.

> Depois de reconhecer um risco, leva alguns minutos para que a alteração seja refletida na lista de sugestões do Digital Advisor.

Não reconhecer riscos

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para desreconhecer qualquer risco que tenha sido reconhecido anteriormente.

Passos

1. No System Manager, exiba a lista de riscos executando o procedimento Ver detalhes dos riscosem .
2. Clique no nome de risco de um risco reconhecido que você deseja desreconhecer.
3. Insira as informações nos seguintes campos:
    - Justificação
    - Comentários
4. Clique em **Cancelar reconhecimento**.

> Depois de desreconhecer um risco, leva alguns minutos para que a alteração seja refletida na lista de sugestões do Digital Advisor.

Insights do System Manager

A partir do ONTAP 9.11,1, o Gerenciador de sistema exibe *insights* que ajudam a otimizar o desempenho e a segurança do seu sistema.

Para visualizar, personalizar e responder a insights, consulte "Obtenha insights para ajudar a otimizar seu sistema"

Insights de capacidade

O System Manager pode exibir os seguintes insights em resposta às condições de capacidade do seu sistema:

Insight	Gravidade	Condição	Correções
As camadas locais não têm espaço	Remediar riscos	Um ou mais níveis locais estão mais de 95% cheios e crescendo rapidamente. Os workloads existentes podem não ser capazes de crescer ou, em casos extremos, os workloads existentes podem ficar sem espaço e falhar.	**Correção recomendada**: Execute uma das seguintes opções. • Limpe a fila de recuperação de volume. • Habilite o provisionamento de thin Provisioning em volumes provisionados espessos para liberar o storage preso. • Mova volumes para outro nível local. • Excluir cópias snapshot desnecessárias. • Exclua diretórios desnecessários ou arquivos nos volumes. • Habilite o Fabric Pool para categorizar os dados na nuvem.
As aplicações não têm espaço	Precisa de atenção	Um ou mais volumes estão mais de 95% cheios, mas não têm o crescimento automático ativado.	**Recomendado**: Ative o crescimento até 150% da capacidade atual. **Outras opções**: • Recupere espaço com a exclusão de cópias Snapshot. • Redimensione os volumes. • Excluir diretórios ou arquivos.
A capacidade do volume FlexGroup é desequilibrada	Otimizar o armazenamento	O tamanho dos volumes constituintes de um ou mais volumes do FlexGroup cresceu de forma desigual ao longo do tempo, levando a um desequilíbrio no uso da capacidade. Se os volumes constituintes ficarem cheios, podem ocorrer falhas de gravação.	**Recomendado**: Rebalanceamento dos volumes FlexGroup.

As VMs de storage estão ficando sem capacidade	Otimizar o armazenamento	Uma ou mais VMs de storage estão perto da capacidade máxima. Você não poderá provisionar mais espaço para volumes novos ou existentes se as VMs de storage alcançarem a capacidade máxima.	**Recomendado**: Se possível, aumente o limite máximo de capacidade da VM de armazenamento.

Insights de segurança

O System Manager pode exibir os seguintes insights em resposta a condições que podem comprometer a segurança de seus dados ou do sistema.

Insight	Gravidade	Condição	Correções
Os volumes ainda estão no modo de aprendizado anti-ransomware	Precisa de atenção	Um ou mais volumes estão no modo de aprendizado anti-ransomware por 90 dias.	**Recomendado**: Ative o modo ativo anti-ransomware para esses volumes.
A exclusão automática de cópias Snapshot está habilitada nos volumes	Precisa de atenção	A eliminação automática de instantâneos está ativada num ou mais volumes.	**Recomendado**: Desative a exclusão automática de cópias Snapshot. Caso contrário, em caso de ataque de ransomware, a recuperação de dados para esses volumes pode não ser possível.
Os volumes não têm políticas Snapshot	Precisa de atenção	Um ou mais volumes não têm uma política de snapshot adequada anexada a eles.	**Recomendado**: Anexe uma política Snapshot a volumes que não tenham um. Caso contrário, em caso de ataque de ransomware, a recuperação de dados para esses volumes pode não ser possível.
FPolicy nativo não está configurado	Prática recomendada	O FPolicy nativo não está configurado em uma ou mais VMs de armazenamento nas.	**Recomendado**: **IMPORTANTE**: Bloquear extensões pode levar a resultados inesperados. A partir de 9.11.1, é possível habilitar o FPolicy nativo para VMs de armazenamento, o que bloqueia mais de 3000 extensões de arquivo conhecidas por serem usadas para ataques de ransomware. "Configurar FPolicy nativo" Nas VMs de armazenamento nas para controlar as extensões de arquivo permitidas ou não permitidas para serem gravadas em volumes em seu ambiente.

O Telnet está ativado	Prática recomendada	O Secure Shell (SSH) deve ser usado para acesso remoto seguro.	**Recomendado**: Desative o Telnet e use SSH para acesso remoto seguro.
Poucos servidores NTP estão configurados	Prática recomendada	O número de servidores configurados para NTP é inferior a 3.	**Recomendado**: Associe pelo menos três servidores NTP ao cluster. Caso contrário, podem ocorrer problemas com a sincronização da hora do cluster.
O Remote Shell (RSH) está ativado	Prática recomendada	O Secure Shell (SSH) deve ser usado para acesso remoto seguro.	**Recomendado**: Desative o RSH e use SSH para acesso remoto seguro.
O banner de login não está configurado	Prática recomendada	As mensagens de login não são configuradas para o cluster, para a VM de armazenamento ou para ambos.	**Recomendado**: Configure os banners de login para o cluster e a VM de armazenamento e habilite seu uso.
O AutoSupport está usando um protocolo não seguro	Prática recomendada	O AutoSupport não está configurado para se comunicar via HTTPS.	**Recomendado**: É altamente recomendável usar HTTPS como protocolo de transporte padrão para enviar mensagens AutoSupport para suporte técnico.
O utilizador de administrador predefinido não está bloqueado	Prática recomendada	Ninguém fez login usando uma conta administrativa padrão (admin ou diag), e essas contas não estão bloqueadas.	**Recomendado**: Bloqueie contas administrativas padrão quando elas não estiverem sendo usadas.
O Secure Shell (SSH) está usando cifras não seguras	Prática recomendada	A configuração atual usa cifras CBC não seguras.	**Recomendado**: Você deve permitir apenas cifras seguras em seu servidor web para proteger a comunicação segura com seus visitantes. Remover cifras que tenham nomes contendo "cbc", como "ais128-cbc", "aes192-cbc", "AES256-cbc" e "3DES-cbc".
A conformidade com o FIPS 140-2 global está desativada	Prática recomendada	A conformidade com o FIPS 140-2 global é desativada no cluster.	**Recomendado**: Por motivos de segurança, você deve habilitar a criptografia compatível com FIPS global 140-2 para garantir que o ONTAP possa se comunicar com segurança com clientes externos ou clientes de servidor.

Os volumes não estão sendo monitorados para ataques de ransomware	Precisa de atenção	O antirransomware é desativado em um ou mais volumes.	**Recomendado**: Ative o anti-ransomware nos volumes. Caso contrário, você pode não notar quando os volumes estão sendo ameaçados ou sob ataque.
As VMs de storage não estão configuradas para anti-ransomware	Prática recomendada	Uma ou mais VMs de storage não estão configuradas para proteção contra ransomware.	**Recomendado**: Ative o anti-ransomware nas VMs de armazenamento. Caso contrário, você pode não notar quando as VMs de armazenamento estão sendo ameaçadas ou sob ataque.

Insights de configuração

O System Manager pode exibir os seguintes insights em resposta a preocupações sobre a configuração do seu sistema.

Insight	Gravidade	Condição	Correções
O cluster não está configurado para notificações	Prática recomendada	E-mail, webhooks ou um traphost SNMP não está configurado para permitir que você receba notificações sobre problemas com o cluster.	**Recomendado**: Configure notificações para o cluster.
O cluster não está configurado para atualizações automáticas.	Prática recomendada	O cluster não foi configurado para receber atualizações automáticas para o pacote de qualificação de disco mais recente, firmware de disco, firmware de gaveta, firmware de SP/BMC ou arquivos de segurança quando estiverem disponíveis.	**Recomendado**: Ative este recurso.

O firmware do cluster não está atualizado	Prática recomendada	O seu sistema não tem a atualização mais recente do firmware, que pode ter melhorias, patches de segurança ou novos recursos que ajudam a proteger o cluster para um melhor desempenho.	**Recomendado**: Atualize o firmware do ONTAP.

Obtenha insights para ajudar a otimizar seu sistema

Com o System Manager, você pode visualizar insights que ajudam a otimizar seu sistema.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para ver os insights que o ajudam a otimizar seu sistema. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A partir do ONTAP 9.11,0, você pode visualizar insights no Gerenciador de sistemas que ajudam a otimizar a conformidade de capacidade e segurança do seu sistema.

A partir do ONTAP 9.11,1, você pode visualizar insights adicionais que ajudam a otimizar a capacidade, a conformidade de segurança e a configuração do seu sistema.

Bloquear extensões pode levar a resultados inesperados. A partir do ONTAP 9.11,1, você pode habilitar o FPolicy nativo para VMs de armazenamento usando o Gerenciador do sistema. Você pode receber uma mensagem do System Manager Insight recomendando que "Configurar FPolicy nativo"você seja uma VM de storage.

Com o FPolicy Native Mode, você pode permitir ou desativar extensões de arquivo específicas. O System Manager recomenda mais de 3000 extensões de arquivos não permitidas que foram usadas em ataques de ransomware anteriores. Algumas dessas extensões podem ser usadas por arquivos legítimos em seu ambiente e bloqueá-las pode levar a problemas inesperados.

Portanto, é altamente recomendável que você modifique a lista de extensões para atender às necessidades do seu ambiente. Consulte a "Como remover uma extensão de arquivo de uma configuração FPolicy nativa criada pelo System Manager usando o System Manager para recriar a diretiva".

Para saber mais sobre FPolicy nativo, "Tipos de configuração Fpolicy"consulte .

Com base nas práticas recomendadas, esses insights são exibidos em uma página a partir da qual você pode iniciar ações imediatas para otimizar seu sistema. Para obter mais detalhes sobre cada insight, "Insights do System Manager"consulte .

Ver insights de otimização

Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.

   A página **Insights** mostra grupos de insights. Cada grupo de insights pode conter um ou mais insights. São apresentados os seguintes grupos:

   - Precisa de sua atenção
   - Remediar riscos
   - Otimizar seu storage

2. (Opcional) filtre os insights exibidos clicando nesses botões no canto superior direito da página:
   -  Exibe os insights relacionados à segurança.
   -  Exibe os insights relacionados à capacidade.
   -  Exibe os insights relacionados à configuração.
   -  Exibe todos os insights.

Responda a insights para otimizar seu sistema

No System Manager, você pode responder a insights descartando-os, explorando diferentes maneiras de corrigir os problemas ou iniciando o processo para corrigir os problemas.

Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. Passe o Mouse sobre um insight para revelar os botões para executar as seguintes ações:
   - **Dismiss**: Remova o insight da visualização. Para "não descartar" a perceção, [customize-settings-insights]consulte .
   - **Explore**: Descubra várias maneiras de remediar o problema mencionado no insight. Este botão aparece apenas se houver mais de um método de correção.
   - **Fix**: Inicie o processo de correção do problema mencionado no insight. Você será solicitado a confirmar se deseja executar a ação necessária para aplicar a correção.

> Algumas dessas ações podem ser iniciadas de outras páginas no System Manager, mas a página **Insights** ajuda você a simplificar suas tarefas diárias, permitindo que você inicie essa ação a partir desta página.

Personalize as configurações para insights

Você pode personalizar quais insights serão notificados no System Manager.

Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. No canto superior direito da página, clique em e selecione **Configurações**.

3. Na página **Configurações**, verifique se há uma seleção nas caixas de seleção ao lado dos insights sobre os quais você deseja ser notificado. Se você descartou anteriormente um insight, você pode "'cancelar o insight', garantindo que uma verificação esteja em sua caixa de seleção.
4. Clique em **Salvar**.

Exporte os insights como um arquivo PDF

Você pode exportar todos os insights aplicáveis como um arquivo PDF.

Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. No canto superior direito da página, clique em e selecione **Exportar**.

Configurar FPolicy nativo

A partir do ONTAP 9.11,1, quando você recebe um Insight do System Manager que sugere a implementação de FPolicy nativo, você pode configurá-lo em suas VMs e volumes de storage.

Antes de começar

Quando você acessa o System Manager Insights, em **aplicar práticas recomendadas**, você pode receber uma mensagem dizendo que o FPolicy nativo não está configurado.

Para saber mais sobre os tipos de configuração FPolicy, "Tipos de configuração FPolicy"consulte .

Passos

1. No System Manager, clique em **Insights** na coluna de navegação à esquerda.
2. Em **aplicar as melhores práticas**, localize **Native FPolicy não está configurado**.
3. Leia a seguinte mensagem antes de tomar medidas:

> **Bloquear extensões pode levar a resultados inesperados.** A partir do ONTAP 9.11,1, você pode habilitar o FPolicy nativo para VMs de armazenamento usando o Gerenciador do sistema. Com o FPolicy Native Mode, você pode permitir ou desativar extensões de arquivo específicas. O System Manager recomenda mais de 3000 extensões de arquivos não permitidas que foram usadas em ataques de ransomware anteriores. Algumas dessas extensões podem ser usadas por arquivos legítimos em seu ambiente e bloqueá-las pode levar a problemas inesperados.
>
> Portanto, é altamente recomendável que você modifique a lista de extensões para atender às necessidades do seu ambiente. Consulte a "Como remover uma extensão de arquivo de uma configuração FPolicy nativa criada pelo System Manager usando o System Manager para recriar a diretiva".

4. Clique em **Fix**.
5. Selecione as VMs de armazenamento às quais você deseja aplicar o FPolicy nativo.
6. Para cada VM de armazenamento, selecione os volumes que receberão o FPolicy nativo.
7. Clique em **Configurar**.

Monitore e gerencie a performance do cluster usando a CLI

Visão geral do gerenciamento e monitoramento de desempenho

Você pode configurar tarefas básicas de monitoramento e gerenciamento de desempenho e identificar e resolver problemas comuns de desempenho.

Você pode usar esses procedimentos para monitorar e gerenciar o desempenho do cluster se as seguintes suposições se aplicarem à sua situação:

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você deseja exibir o status e os alertas do sistema, monitorar o desempenho do cluster e realizar análises de causa-raiz usando o Active IQ Unified Manager (antigo Gerenciador Unificado de OnCommand), além da interface de linha de comando do ONTAP.
- Você está usando a interface de linha de comando ONTAP para configurar a qualidade do serviço (QoS) de storage. QoS também está disponível através do seguinte:
  - System Manager
  - API REST do ONTAP
  - Ferramentas do ONTAP para VMware vSphere
  - Gerenciador de nível de Serviço (NetApp)
  - OnCommand Workflow Automation (WFA)
- Você deseja instalar o Unified Manager usando um dispositivo virtual, em vez de uma instalação baseada no Linux ou no Windows.
- Você está disposto a usar uma configuração estática em vez de DHCP para instalar o software.
- Pode aceder aos comandos ONTAP no nível avançado de privilégios.
- Você é um administrador de cluster com a função "admin".

Informações relacionadas

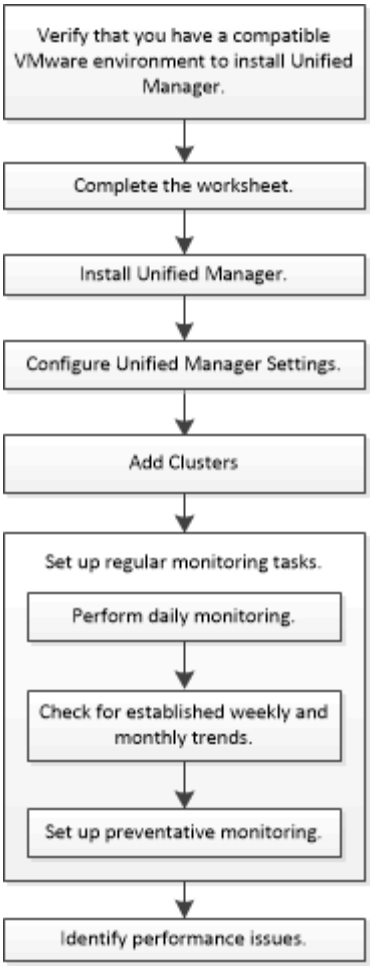
Se essas suposições não estiverem corretas para sua situação, você deverá ver os seguintes recursos:

- "Instalação do Active IQ Unified Manager 9,8"
- "Administração do sistema"

Monitorar o desempenho

Visão geral do fluxo de trabalho de manutenção e monitoramento de desempenho

O monitoramento e a manutenção do desempenho do cluster envolvem a instalação do software Active IQ Unified Manager, a configuração de tarefas básicas de monitoramento, a identificação de problemas de desempenho e a realização de ajustes conforme necessário.



Verifique se seu ambiente VMware é compatível

Para instalar o Active IQ Unified Manager com êxito, você deve verificar se o ambiente VMware atende aos requisitos necessários.

Passos

1. Verifique se sua infraestrutura VMware atende aos requisitos de dimensionamento para a instalação do Unified Manager.
2. Vá para a "Matriz de interoperabilidade" para verificar se você tem uma combinação suportada dos seguintes componentes:
   - Versão de ONTAP
   - Versão do sistema operacional ESXi
   - Versão do VMware vCenter Server
   - Versão do VMware Tools
   - Tipo e versão do navegador

   A Matriz de interoperabilidade lista as configurações suportadas do Unified Manager.
3. Clique no nome da configuração selecionada.

   Os detalhes dessa configuração são exibidos na janela Detalhes da configuração.

4. Revise as informações nas guias a seguir:
   - Notas

     Lista alertas importantes e informações específicas à sua configuração.

   - Políticas e Diretrizes

     Fornece diretrizes gerais para todas as configurações.

Folha de cálculo do Active IQ Unified Manager

Antes de instalar, configurar e conetar o Active IQ Unified Manager, você deve ter informações específicas sobre seu ambiente prontamente disponíveis. Pode registar as informações na folha de trabalho.

Informações de instalação do Unified Manager

Máquina virtual na qual o software é implantado	O seu valor
Endereço IP do servidor ESXi	
Host nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	
Endereço DNS primário	
Endereço DNS secundário	
Pesquisar domínios	
Nome de utilizador de manutenção	
Palavra-passe do utilizador de manutenção	

Informações de configuração do Unified Manager

Definição	O seu valor
Endereço de e-mail do usuário de manutenção	
Servidor NTP	

Nome do host do servidor SMTP ou endereço IP	
Nome de utilizador SMTP	
Palavra-passe SMTP	
Porta padrão SMTP	25 (valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome distinto de ligação LDAP	
Palavra-passe LDAP BIND	
Nome de administrador do ative Directory	
Palavra-passe do ative Directory	
Nome distinto da base do servidor de autenticação	
Nome do host ou endereço IP do servidor de autenticação	

Informações do cluster

Capture as informações a seguir para cada cluster no Unified Manager.

Cluster 1 de N	O seu valor
Nome do host ou endereço IP de gerenciamento de cluster	
Nome de usuário do administrador do ONTAP O administrador deve ter sido atribuído a função "admin".	
Senha do administrador do ONTAP	
Protocolo (HTTP ou HTTPS)	

Informações relacionadas

"Autenticação de administrador e RBAC"

Instale o Active IQ Unified Manager

Baixe e implante o Active IQ Unified Manager

Para instalar o software, você deve baixar o arquivo de instalação do dispositivo virtual (VA) e usar um cliente VMware vSphere para implantar o arquivo em um servidor VMware ESXi. O VA está disponível num ficheiro OVA.

Passos

1. Vá para a página **Download de software do site de suporte da NetApp** e localize o Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Selecione **VMware vSphere** no menu suspenso **Select Platform** e clique em **Go!**
3. Salve o arquivo "OVA" em um local local ou de rede acessível ao cliente VMware vSphere.
4. No VMware vSphere Client, clique em **File** > **Deploy OVF Template**.
5. Localize o arquivo "OVA" e use o assistente para implantar o dispositivo virtual no servidor ESXi.

   Você pode usar a guia **Propriedades** no assistente para inserir suas informações de configuração estática.

6. Ligue a VM.
7. Clique na guia **Console** para exibir o processo de inicialização inicial.
8. Siga o prompt para instalar o VMware Tools na VM.
9. Configure o fuso horário.
10. Introduza um nome de utilizador e uma palavra-passe de manutenção.
11. Vá para o URL exibido pelo console da VM.

Configure as definições iniciais do Active IQ Unified Manager

A caixa de diálogo Configuração inicial do Active IQ Unified Manager é exibida quando você acessa pela primeira vez a IU da Web, o que permite configurar algumas configurações iniciais e adicionar clusters.

Passos

1. Aceite a configuração padrão AutoSupport Enabled.
2. Insira os detalhes do servidor NTP, o endereço de e-mail do usuário de manutenção, o nome do host do servidor SMTP e opções SMTP adicionais e clique em **Salvar**.

Depois de terminar

Quando a configuração inicial estiver concluída, a página fontes de dados do cluster é exibida onde você pode adicionar os detalhes do cluster.

Especifique os clusters a serem monitorados

Você deve adicionar um cluster a um servidor Active IQ Unified Manager para monitorar o cluster, exibir o status de descoberta do cluster e monitorar seu desempenho.

O que você vai precisar

- Você deve ter as seguintes informações:
  - Nome do host ou endereço IP de gerenciamento de cluster

    O nome do host é o nome de domínio totalmente qualificado (FQDN) ou o nome abreviado que o Unified Manager usa para se conetar ao cluster. Esse nome de host deve ser resolvido para o endereço IP de gerenciamento de cluster.

  O endereço IP de gerenciamento de cluster deve ser o LIF de gerenciamento de cluster da máquina virtual de storage administrativo (SVM). Se você usar um LIF de gerenciamento de nós, a operação falhará.

  - Nome de usuário e senha do administrador do ONTAP
  - Tipo de protocolo (HTTP ou HTTPS) que pode ser configurado no cluster e o número da porta do cluster
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- O administrador do ONTAP deve ter as funções de administrador ONTAPI e SSH.
- O FQDN do Gerenciador Unificado deve ser capaz de fazer ping no ONTAP.

  Você pode verificar isso usando o comando ONTAP `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

Sobre esta tarefa

Para uma configuração do MetroCluster, você deve adicionar clusters locais e remotos, e os clusters devem estar configurados corretamente.

Passos

1. Clique em **Configuration** > **Cluster Data Sources**.
2. Na página clusters, clique em **Add**.
3. Na caixa de diálogo **Adicionar cluster**, especifique os valores necessários, como o nome do host ou o endereço IP (IPv4 ou IPv6) do cluster, nome de usuário, senha, protocolo de comunicação e número da porta.

   Por predefinição, o protocolo HTTPS é selecionado.

   Você pode alterar o endereço IP de gerenciamento de cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP é refletido na grade do cluster e na página de configuração do cluster após o próximo ciclo de monitoramento terminar.

4. Clique em **Add**.
5. Se o HTTPS estiver selecionado, execute as seguintes etapas:

   a. Na caixa de diálogo **autorizar Host**, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.

   b. Clique em **Sim**.

      O Unified Manager verifica o certificado somente quando o cluster é adicionado inicialmente, mas não o verifica para cada chamada de API para o ONTAP.

   Se o certificado expirou, não é possível adicionar o cluster. Você deve renovar o certificado SSL e, em

seguida, adicionar o cluster.

6. **Opcional**: Veja o status de descoberta do cluster:

   a. Revise o status de deteção de cluster na página **Configuração de cluster**.

   O cluster é adicionado ao banco de dados do Unified Manager após o intervalo de monitoramento padrão de aproximadamente 15 minutos.

Configure tarefas básicas de monitoramento

Realize a monitorização diária

Você pode executar o monitoramento diário para garantir que não tenha problemas imediatos de desempenho que exijam atenção.

Passos

1. Na IU do Active IQ Unified Manager, vá para a página **Inventário de Eventos** para ver todos os eventos atuais e obsoletos.
2. Na opção **View**, `Active Performance Events` selecione e determine qual ação é necessária.

Use tendências de desempenho semanais e mensais para identificar problemas de desempenho

Identificar tendências de desempenho pode ajudá-lo a identificar se o cluster está sendo usado em excesso ou subusado analisando a latência do volume. Você pode usar etapas semelhantes para identificar gargalos de CPU, rede ou outros sistemas.

Passos

1. Localize o volume que você suspeita estar sendo subutilizado ou sobreusado.
2. Na guia **Detalhes do volume**, clique em **30 d** para exibir os dados históricos.
3. No menu suspenso "dividir dados por", selecione **latência** e clique em **Enviar**.
4. Desmarque **Aggregate** no gráfico de comparação de componentes de cluster e compare a latência do cluster com o gráfico de latência de volume.
5. Selecione **agregar** e desmarque todos os outros componentes no gráfico de comparação de componentes de cluster e, em seguida, compare a latência agregada com o gráfico de latência de volume.
6. Compare o gráfico de latência de leitura/gravação com o gráfico de latência de volume.
7. Determinar se os workloads de aplicações cliente causaram uma contenção de workload e rebalancear os workloads conforme necessário.
8. Determine se o agregado é usado demais e cause contenção e rebalancear os workloads conforme necessário.

Use limites de performance para gerar notificações de eventos

Eventos são notificações que o Active IQ Unified Manager gera automaticamente quando ocorre uma condição predefinida ou quando um valor de contador de desempenho cruza um limite. Os eventos ajudam a identificar problemas de desempenho nos clusters que você está monitorando. Você pode configurar alertas para enviar notificações por e-mail automaticamente quando ocorrerem eventos de determinados tipos de gravidade.

Definir limites de desempenho

Você pode definir limites de desempenho para monitorar problemas críticos de performance. Os limites definidos pelo usuário acionam um aviso ou uma notificação de evento crítico quando o sistema se aproxima ou excede o limite definido.

Passos

1. Crie os limites de aviso e evento crítico:
   a. Selecione **Configuração** > **limites de desempenho**.
   b. Clique em **criar**.
   c. Selecione o tipo de objeto e especifique um nome e uma descrição da política.
   d. Selecione a condição do contador de objetos e especifique os valores limite que definem eventos de aviso e crítico.
   e. Selecione a duração do tempo em que os valores-limite devem ser violados para que um evento seja enviado e clique em **Salvar**.
2. Atribua a política de limite ao objeto de storage.
   a. Vá para a página Inventário para o mesmo tipo de objeto de cluster que você selecionou anteriormente e escolha **desempenho** na opção Exibir.
   b. Selecione o objeto ao qual você deseja atribuir a política de limite e clique em **Assign Threshold Policy**.
   c. Selecione a política criada anteriormente e clique em **Assign Policy**.

Exemplo

Você pode definir limites definidos pelo usuário para saber mais sobre problemas críticos de desempenho. Por exemplo, se você tem um Microsoft Exchange Server e sabe que ele falha se a latência do volume exceder 20 milissegundos, você pode definir um limite de aviso em 12 milissegundos e um limite crítico em 15 milissegundos. Com essa configuração de limite, você pode receber notificações quando a latência do volume exceder o limite.

Adicionar alertas

Você pode configurar alertas para notificá-lo quando um evento específico é gerado. Você pode configurar alertas para um único recurso, para um grupo de recursos ou para eventos de um tipo de gravidade específico. Você pode especificar a frequência com que deseja ser notificado e associar um script ao alerta.

O que você vai precisar

- Você deve ter configurado configurações de notificação, como endereço de e-mail do usuário, servidor SMTP e host de intercetação SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento é gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta e os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, você deve ter adicionado o script ao

Unified Manager usando a página Scripts.

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Sobre esta tarefa

Você pode criar um alerta diretamente da página de detalhes do evento depois de receber um evento, além de criar um alerta na página Configuração de Alerta, conforme descrito aqui.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de alerta**.
2. Na página **Configuração de alerta**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **recursos** e selecione os recursos a serem incluídos ou excluídos do alerta.

   Você pode definir um filtro especificando uma cadeia de texto no campo **Name contains** para selecionar um grupo de recursos. Com base na cadeia de texto especificada, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto especificada é sensível a maiúsculas e minúsculas.

   Se um recurso estiver em conformidade com as regras incluir e excluir que você especificou, a regra excluir terá precedência sobre a regra incluir e o alerta não será gerado para eventos relacionados ao recurso excluído.

5. Clique em **Eventos** e selecione os eventos com base no nome do evento ou no tipo de gravidade do evento para os quais deseja acionar um alerta.

   Para selecionar mais de um evento, pressione a tecla Ctrl enquanto você faz suas seleções.

6. Clique em **ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, escolha se uma trap SNMP será enviada ao recetor de trap e atribua um script a ser executado quando um alerta for gerado.

   Se você modificar o endereço de e-mail especificado para o usuário e reabrir o alerta para edição, o campo Nome será exibido em branco porque o endereço de e-mail modificado não será mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificou o endereço de e-mail do usuário selecionado na página usuários, o endereço de e-mail modificado não será atualizado para o usuário selecionado.

   Você também pode optar por notificar os usuários através de traps SNMP.

7. Clique em **Salvar**.

Exemplo de adição de um alerta

Este exemplo mostra como criar um alerta que atenda aos seguintes requisitos:

- Nome do alerta: HealthTest
- Recursos: Inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: Inclui todos os eventos críticos de saúde

- Ações: Inclui "sample@domain.com", um script "Test", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

1. Clique em **Nome** e insira `HealthTest` no campo **Nome** do alerta.
2. Clique em **recursos** e, na guia incluir, selecione **volumes** na lista suspensa.
   a. Digite `abc` o campo **Name contains** para exibir os volumes cujo nome contém "abc".
   b. Selecione *[All Volumes whose name contains 'abc'] na área recursos disponíveis e mova-o para a área recursos selecionados.
   c. Clique em **Excluir**, digite `xyz` o campo **Nome contém** e clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítica** no campo gravidade do evento.
4. Selecione **todos os Eventos críticos** na área Eventos correspondentes e mova-os para a área Eventos selecionados.
5. Clique em **ações** e insira `sample@domain.com` no campo alertar esses usuários.
6. Selecione **lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

   Você pode configurar um alerta para enviar repetidamente notificações aos destinatários por um tempo especificado. Você deve determinar a hora a partir da qual a notificação de evento está ativa para o alerta.
7. No menu Selecionar Script para execução, selecione **Test** script.
8. Clique em **Salvar**.

Configure as definições de alerta

Você pode especificar quais eventos do Active IQ Unified Manager acionam alertas, os destinatários de e-mail desses alertas e a frequência dos alertas.

O que você vai precisar

Tem de ter a função Administrador de aplicações.

Sobre esta tarefa

Você pode configurar configurações de alerta exclusivas para os seguintes tipos de eventos de desempenho:

- Eventos críticos desencadeados por violações de limites definidos pelo usuário
- Eventos de aviso acionados por violações de limites definidos pelo usuário, limites definidos pelo sistema ou limites dinâmicos

Por padrão, os alertas de e-mail são enviados aos usuários administrativos do Unified Manager para todos os novos eventos. Você pode enviar alertas por e-mail para outros usuários adicionando os endereços de e-mail desses usuários.

> Para desativar o envio de alertas para determinados tipos de eventos, você deve desmarcar todas as caixas de seleção de uma categoria de evento. Esta ação não impede que os eventos apareçam na interface do utilizador.

Passos

1. No painel de navegação esquerdo, selecione **Gerenciamento de armazenamento** > **Configuração de alerta**.

É apresentada a página Configuração de alerta.

2. Clique em **Add** e configure as configurações apropriadas para cada um dos tipos de evento.

   Para enviar alertas de e-mail para vários usuários, insira uma vírgula entre cada endereço de e-mail.

3. Clique em **Salvar**.

Identificar problemas de desempenho no Active IQ Unified Manager

Se ocorrer um evento de desempenho, você poderá localizar a origem do problema no Active IQ Unified Manager e usar outras ferramentas para corrigi-lo. Você pode receber uma notificação por e-mail de um evento ou notar o evento durante o monitoramento diário.

Passos

1. Clique no link na notificação por e-mail, que o leva diretamente ao objeto de armazenamento com um evento de desempenho.

Se você…	Então…
Receba uma notificação por e-mail de um evento	Clique no link para ir diretamente para a página de detalhes do evento.
Observe o evento enquanto analisa a página Inventário de Eventos	Selecione o evento para ir diretamente para a página de detalhes do evento.

2. Se o evento tiver cruzado um limite definido pelo sistema, siga as ações sugeridas na IU para solucionar o problema.
3. Se o evento tiver atravessado um limite definido pelo usuário, analise o evento para determinar se você precisa agir.
4. Se o problema persistir, verifique as seguintes definições:
   - Definições de protocolo no sistema de armazenamento
   - Configurações de rede em qualquer Ethernet ou switch de malha
   - Definições de rede no sistema de armazenamento
   - Layout de disco e métricas agregadas no sistema de storage
5. Se o problema persistir, contacte o suporte técnico para obter assistência.

Use o Digital Advisor para visualizar o desempenho do sistema

Para qualquer sistema ONTAP que envie telemetria de AutoSupport para o NetApp, é possível visualizar dados abrangentes de desempenho e capacidade. O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no System Manager.

Você pode visualizar gráficos de utilização da CPU, latência, IOPS, IOPS por protocolo e taxa de transferência de rede. Você também pode baixar esses dados no formato .csv para análise em outras ferramentas.

Além desses dados de performance, o Digital Advisor mostra a eficiência de storage por workload e compara essa eficiência com a eficiência esperada para esse tipo de workload. Você pode ver as tendências de capacidade e ver uma estimativa de quanto storage adicional você pode precisar adicionar em um determinado período de tempo.

- A eficiência de storage está disponível no nível do cliente, do cluster e do nó, no lado esquerdo do painel principal.
- O desempenho está disponível no nível do cluster e do nó no lado esquerdo do painel principal.

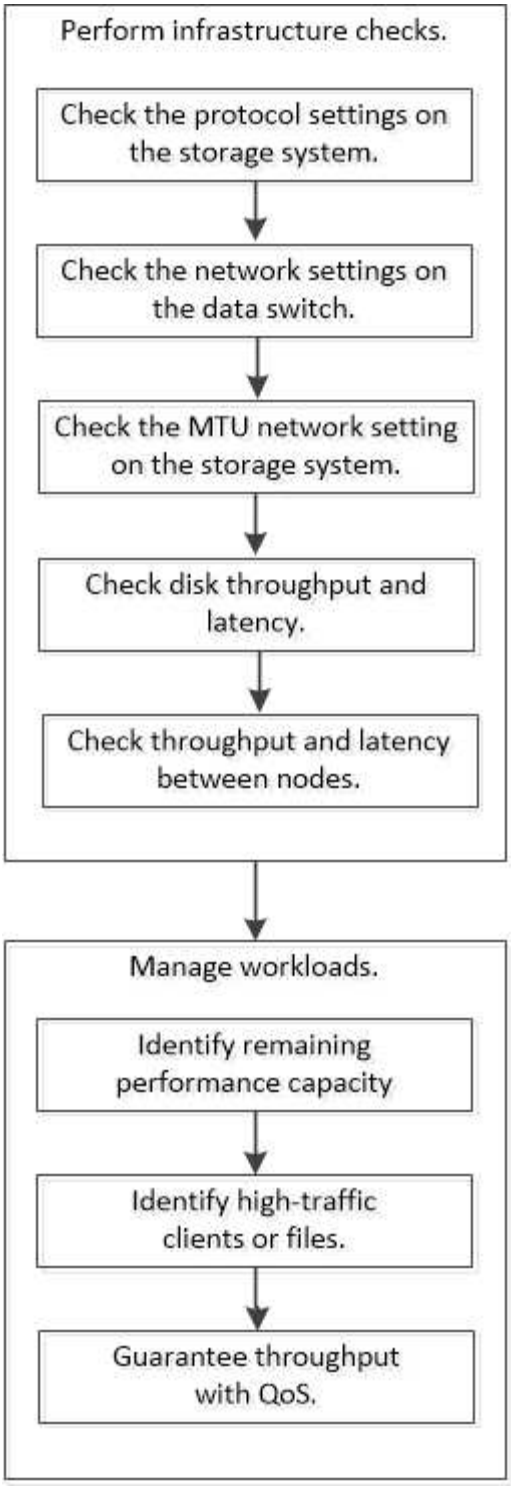
Informações relacionadas

- "Documentação do Digital Advisor"
- "Lista de reprodução de vídeo do Digital Advisor"
- "Portal Web do Digital Advisor"

Gerenciar problemas de performance

Fluxo de trabalho de gerenciamento de desempenho

Depois de identificar um problema de desempenho, você poderá realizar algumas verificações básicas de diagnóstico de sua infraestrutura para descartar erros óbvios de configuração. Se eles não identificarem o problema, você pode começar a analisar problemas de gerenciamento de workload.



Realizar verificações básicas de infraestrutura

Verifique as definições do protocolo no sistema de armazenamento

Verifique o tamanho máximo de transferência TCP NFS

Para NFS, você pode verificar se o tamanho máximo de transferência TCP para leituras e gravações pode estar causando um problema de desempenho. Se você acha que o tamanho está diminuindo o desempenho, você pode aumentá-lo.

O que você vai precisar

- Você deve ter o administrador de cluster Privileges para executar esta tarefa.
- Tem de utilizar comandos avançados de nível de privilégio para esta tarefa.

Passos

1. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Verifique o tamanho máximo de transferência TCP:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. Se o tamanho máximo de transferência TCP for muito pequeno, aumente o tamanho:

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. Voltar ao nível de privilégio administrativo:

   ```
   set -privilege admin
   ```

Exemplo

O exemplo a seguir altera o tamanho máximo de transferência TCP de `SVM1` para 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

Verifique o tamanho de leitura/gravação iSCSI TCP

Para iSCSI, você pode verificar o tamanho de leitura/gravação TCP para determinar se a configuração de tamanho está criando um problema de desempenho. Se o tamanho for a origem de um problema, você pode corrigi-lo.

O que você vai precisar

São necessários comandos avançados de nível de privilégio para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Verifique a configuração de tamanho da janela TCP:

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. Modifique a configuração de tamanho da janela TCP:

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. Retornar ao privilégio administrativo:

```
set -privilege admin
```

Exemplo

O exemplo a seguir altera o tamanho da janela TCP `SVM1` para 131.400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

Verificar as definições multiplexadas CIFS

Se o desempenho lento da rede CIFS causar um problema de desempenho, pode modificar as definições multiplexadas para melhorá-las e corrigi-las.

Passos

1. Verificar a definição multiplexada CIFS:

   `vserver cifs options show -vserver -vserver_name -instance`

2. Modificar a definição multiplexada CIFS:

   `vserver cifs options modify –vserver -vserver_name –max-mpx integer`

Exemplo

O exemplo seguinte altera a contagem multiplexada máxima `SVM1` para 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

Verifique a velocidade da porta do adaptador FC

A velocidade da porta de destino do adaptador deve corresponder à velocidade do dispositivo ao qual se coneta, para otimizar o desempenho. Se a porta estiver definida para negociação automática, pode demorar mais tempo para se reconetar após uma tomada de posse e giveback ou outra interrupção.

O que você vai precisar

Todos os LIFs que usam esse adaptador como porta inicial devem estar offline.

Passos

1. Coloque o adaptador offline:

   `network fcp adapter modify -node nodename -adapter adapter -state down`

2. Verifique a velocidade máxima do adaptador de porta:

   `fcp adapter show -instance`

3. Altere a velocidade da porta, se necessário:

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Coloque o adaptador online:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Coloque todos os LIFs no adaptador online:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

Exemplo

O exemplo a seguir altera a velocidade da porta do adaptador `0d node1` para 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

Verifique as definições de rede nos interrutores de dados

Embora seja necessário manter as mesmas configurações de MTU em seus clientes, servidores e sistemas de armazenamento (ou seja, endpoints de rede), os dispositivos de rede intermediários, como NICs e switches, devem ser definidos para seus valores máximos de MTU para garantir que o desempenho não seja afetado.

Para obter o melhor desempenho, todos os componentes da rede devem poder encaminhar quadros jumbo (9000 bytes IP, 9022 bytes incluindo Ethernet). Os switches de dados devem ser definidos para pelo menos 9022 bytes, mas um valor típico de 9216 é possível com a maioria dos switches.

Procedimento

Para centrais de dados, verifique se o tamanho da MTU está definido para 9022 ou superior.

Para obter mais informações, consulte a documentação do fornecedor do switch.

Verifique a configuração de rede MTU no sistema de armazenamento

Você pode alterar as configurações de rede no sistema de armazenamento se elas não forem as mesmas do cliente ou de outros endpoints de rede. Enquanto a configuração MTU da rede de gerenciamento está definida como 1500, o tamanho da MTU da rede de dados deve ser 9000.

Sobre esta tarefa

Todas as portas dentro de um domínio de broadcast têm o mesmo tamanho MTU, com exceção do tráfego de gerenciamento de gerenciamento de gerenciamento de portas e0M. Se a porta for parte de um domínio de broadcast, use o `broadcast-domain modify` comando para alterar a MTU para todas as portas dentro do domínio de broadcast modificado.

Observe que os dispositivos de rede intermediários, como NICs e switches de dados, podem ser definidos para tamanhos de MTU mais altos do que os endpoints de rede. Para obter mais informações, "Verifique as definições de rede nos interrutores de dados"consulte .

Passos

1. Verifique a configuração da porta MTU no sistema de armazenamento:

   ```
   network port show -instance
   ```

2. Altere a MTU no domínio de broadcast usado pelas portas:

   ```
   network port broadcast-domain modify -ipspace ipspace -broadcast-domain
   broadcast_domain -mtu new _mtu
   ```

Exemplo

O exemplo a seguir altera a configuração da porta MTU para 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

Verifique a taxa de transferência e a latência do disco

Você pode verificar a taxa de transferência de disco e as métricas de latência dos nós de cluster para ajudá-lo na solução de problemas.

Sobre esta tarefa

São necessários comandos avançados de nível de privilégio para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Verifique as métricas de taxa de transferência e latência do disco:

   ```
   statistics disk show -sort-key latency
   ```

Exemplo

O exemplo a seguir exibe os totais em cada operação de leitura ou gravação do usuário para `node2` On `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Verifique a taxa de transferência e a latência entre nós

Você pode usar o `network test-path` comando para identificar gargalos de rede ou para pré-qualificar caminhos de rede entre nós. Você pode executar o comando entre nós ou nós entre clusters.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários comandos avançados de nível de privilégio para esta tarefa.
- Para um caminho entre clusters, os clusters de origem e destino devem ser peered.

Sobre esta tarefa

Ocasionalmente, o desempenho da rede entre nós pode não atender às expetativa de configuração do caminho. Uma taxa de transmissão de 1 Gbps para o tipo de grandes transferências de dados vistas nas operações de replicação do SnapMirror, por exemplo, não seria consistente com um link de 10 GbE entre os clusters de origem e destino.

Você pode usar o `network test-path` comando para medir a taxa de transferência e a latência entre nós. Você pode executar o comando entre nós ou nós entre clusters.

> O teste satura o caminho da rede com dados, então você deve executar o comando quando o sistema não estiver ocupado e quando o tráfego de rede entre nós não for excessivo. O teste expira após dez segundos. O comando só pode ser executado entre nós ONTAP 9.

A `session-type` opção identifica o tipo de operação que você está executando sobre o caminho da rede - por exemplo, "AsyncMirrorRemote" para replicação do SnapMirror para um destino remoto. O tipo determina a quantidade de dados utilizados no teste. A tabela a seguir define os tipos de sessão:

Tipo de sessão	Descrição
AsyncMirrorLocal	Configurações usadas pelo SnapMirror entre nós no mesmo cluster

AsyncMirrorRemote	Configurações usadas pelo SnapMirror entre nós em clusters diferentes (tipo padrão)
RemoteDataTransfer	Configurações usadas pelo ONTAP para acesso remoto a dados entre nós no mesmo cluster (por exemplo, uma solicitação NFS para um nó para um arquivo armazenado em um volume em um nó diferente)

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Meça a taxa de transferência e a latência entre nós:

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   O nó de origem deve estar no cluster local. O nó de destino pode estar no cluster local ou em um cluster com peering. Um valor de "local" para `-source-node` especifica o nó no qual você está executando o comando.

   O comando a seguir mede a taxa de transferência e a latência para operações de replicação do tipo SnapMirror entre `node1` no cluster local e `node3` no `cluster2`:

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   ```

   Saída de amostra (os detalhes de saída podem variar dependendo da sua versão do ONTAP):

   ```
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   ```

3. Retornar ao privilégio administrativo:

   ```
   set -privilege admin
   ```

Depois de terminar

Se o desempenho não atender às expetativa de configuração do caminho, você deve verificar as estatísticas de desempenho do nó, usar as ferramentas disponíveis para isolar o problema na rede, verificar as configurações do switch e assim por diante.

Gerenciar workloads

Identificar a capacidade de performance restante

A capacidade de desempenho, ou *headroom*, mede quanto trabalho você pode colocar em um nó ou agregado antes que o desempenho das cargas de trabalho no recurso comece a ser afetado pela latência. Conhecer a capacidade de performance disponível no cluster ajuda você a provisionar e equilibrar workloads.

O que você vai precisar

São necessários comandos avançados de nível de privilégio para esta tarefa.

Sobre esta tarefa

Você pode usar os seguintes valores para a `-object` opção de coletar e exibir estatísticas de headroom:

- Para CPUs, `resource_headroom_cpu`.
- Para agregados `resource_headroom_aggr`, .

Você também pode concluir esta tarefa usando o Gerenciador de sistema e o Active IQ Unified Manager.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Iniciar a coleção de estatísticas de headroom em tempo real:

   ```
   statistics start –object resource_headroom_cpu|aggr
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

3. Apresentar informações estatísticas em tempo real do espaço livre:

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   Para obter a sintaxe completa do comando, consulte a página man.

4. Retornar ao privilégio administrativo:

   ```
   set -privilege admin
   ```

Exemplo

O exemplo a seguir exibe as estatísticas médias horárias do espaço livre para nós de cluster.

Você pode calcular a capacidade de desempenho disponível para um nó subtraindo o `current_utilization` contador do `optimal_point_utilization` contador. Neste exemplo, a capacidade de utilização para `CPU_sti2520-213` é de -14% (72%-86%), o que sugere que a CPU foi superutilizada em média na última hora.

Pode ter especificado `ewma_daily`, `ewma_weekly` ou `ewma_monthly` obter a mesma média das informações durante períodos de tempo mais longos.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                 current_utilization                               86
                   optimal_point_ops                             2573
               optimal_point_latency                             3589
            optimal_point_utilization                              72
     optimal_point_confidence_factor                                1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                 current_utilization                                0
                   optimal_point_ops                                0
               optimal_point_latency                                0
            optimal_point_utilization                              71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

Identificar clientes ou arquivos de alto tráfego

Você pode usar a tecnologia ONTAP ative Objects para identificar clientes ou arquivos responsáveis por uma quantidade desproporcionalmente grande de tráfego de cluster. Depois de identificar esses "principais" clientes ou arquivos, você pode reequilibrar as cargas de trabalho do cluster ou tomar outras medidas para resolver o problema.

O que você vai precisar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Veja os principais clientes que acessam o cluster:

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O comando a seguir exibe os principais clientes acessando `cluster1`:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                          *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. Veja os principais arquivos acessados no cluster:

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Para obter a sintaxe completa do comando, consulte a página man.

   O comando a seguir exibe os principais arquivos acessados no `cluster1`:

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Garantir taxa de transferência com QoS

Garanta a taxa de transferência com uma visão geral de QoS

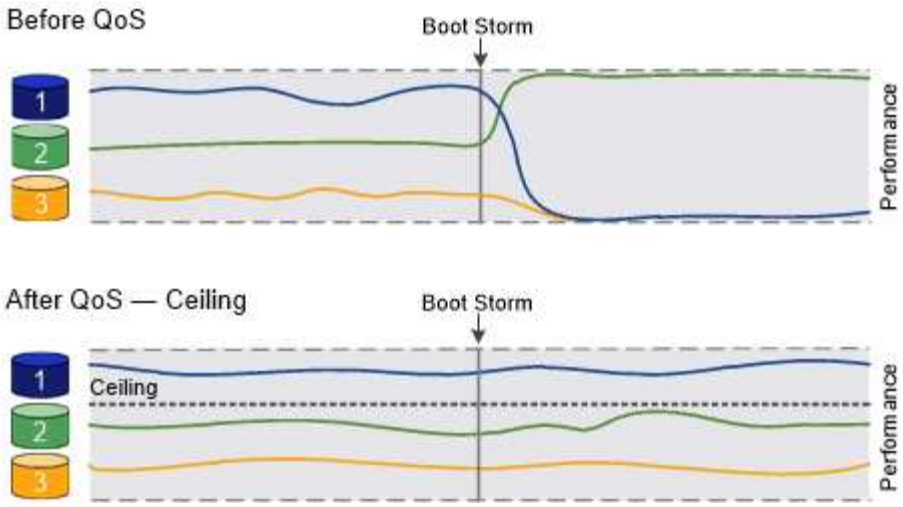
Use a qualidade do serviço (QoS) de storage para garantir que a performance de workloads essenciais não seja degradada pelos workloads da concorrência. Você pode definir um throughput *ceiling* em uma carga de trabalho concorrente para limitar seu impactos nos recursos do sistema ou definir um throughput *floor* para uma carga de trabalho crítica, garantindo que ele atenda aos objetivos mínimos de taxa de transferência, independentemente da demanda por cargas de trabalho concorrentes. Você pode até mesmo definir um teto e piso para a mesma carga de trabalho.

Sobre limites máximos de taxa de transferência (QoS Max)

Um limite máximo de taxa de transferência limita a taxa de transferência de um workload a um número máximo de IOPS ou Mbps, ou IOPS e Mbps. Na figura abaixo, o limite de taxa de transferência para a carga de trabalho 2 garante que não "bully" as cargas de trabalho 1 e 3.

Um *grupo de políticas* define o limite máximo de taxa de transferência para uma ou mais cargas de trabalho. Um workload representa as operações de e/S de um *objeto de storage:* um volume, arquivo, qtree ou LUN, ou todos os volumes, arquivos, qtrees ou LUNs em um SVM. Você pode especificar o limite máximo ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.

> A taxa de transferência para workloads pode exceder o limite máximo especificado em até 10%, especialmente se um workload sofrer mudanças rápidas na taxa de transferência. O teto pode ser excedido em até 50% para lidar com explosões. As explosões ocorrem em nós únicos quando os tokens acumulam até 150%



Sobre os andares de taxa de transferência (QoS min)

Um piso de taxa de transferência garante que a taxa de transferência para um workload não fique abaixo de um número mínimo de IOPS ou Mbps, ou IOPS e Mbps. Na figura abaixo, os andares de taxa de transferência para o workload 1 e o workload 3 garantem que eles atendam aos destinos mínimos de taxa de transferência, independentemente da demanda por workload 2.

Como os exemplos sugerem, um teto de throughput limita a taxa de transferência diretamente. Um piso de taxa de transferência mantém a taxa de transferência indiretamente, dando prioridade às cargas de trabalho para as quais o piso foi definido.

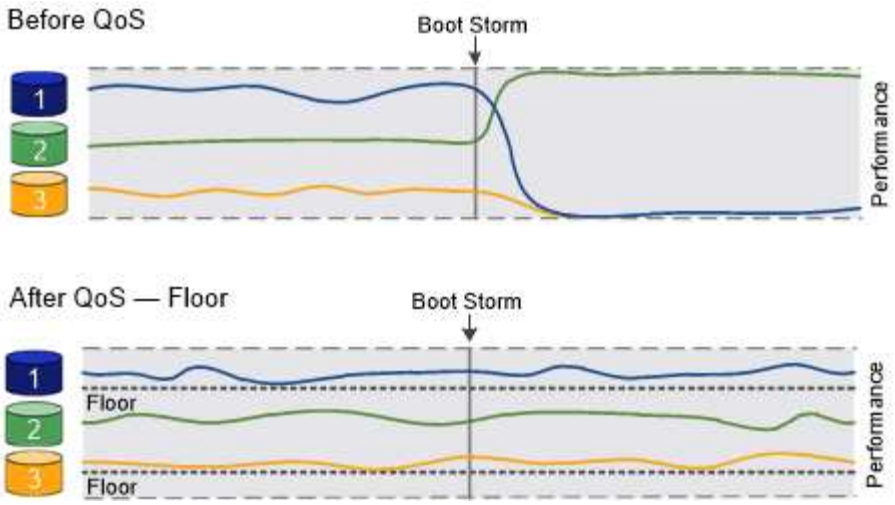
Você pode especificar o piso ao criar o grupo de políticas ou esperar até que você monitore cargas de trabalho para especificá-lo.

A partir do ONTAP 9.13,1, é possível definir os andares de taxa de transferência no escopo da SVM com [adaptive-qos-templates]. Nas versões do ONTAP anteriores a 9.13.1, um grupo de políticas que define uma área de taxa de transferência não pode ser aplicado a um SVM.

Nos lançamentos anteriores ao ONTAP 9.7, os pisos de taxa de transferência são garantidos quando há capacidade de desempenho suficiente disponível.

No ONTAP 9.7 e posterior, os andares de throughput podem ser garantidos mesmo quando há capacidade de desempenho insuficiente disponível. Este novo comportamento do piso é chamado de pisos v2. Para atender às garantias, o piso v2 pode resultar em maior latência em cargas de trabalho sem uma taxa de transferência ou no trabalho que exceda as configurações básicas. Os pisos v2 aplicam-se a QoS e QoS adaptável.

A opção de ativar/desativar o novo comportamento dos pisos v2 está disponível no ONTAP 9.7P6 e posterior. Uma carga de trabalho pode ficar abaixo do nível especificado durante operações críticas como `volume move trigger-cutover`. Mesmo quando a capacidade suficiente está disponível e as operações críticas não estão ocorrendo, a taxa de transferência para uma carga de trabalho pode ficar abaixo do piso especificado em até 5%. Se os andares forem superprovisionados e não houver capacidade de performance, alguns workloads podem ficar abaixo do andar especificado.



Sobre grupos de políticas de QoS compartilhados e não compartilhados

A partir do ONTAP 9.4, você pode usar um grupo de políticas de QoS *não compartilhado* para especificar que o limite ou o piso da taxa de transferência definido se aplica a cada workload de membro individualmente. O comportamento dos grupos de políticas *shared* depende do tipo de política:

- Para limites máximos de taxa de transferência, a taxa de transferência total para as cargas de trabalho atribuídas ao grupo de políticas partilhadas não pode exceder o limite máximo especificado.
- Para andares de taxa de transferência, o grupo de políticas compartilhadas pode ser aplicado somente a um único workload.

Sobre a QoS adaptável

Normalmente, o valor do grupo de políticas que você atribui a um objeto de storage é fixo. Você precisa alterar o valor manualmente quando o tamanho do objeto de armazenamento muda. Um aumento na quantidade de espaço usado em um volume, por exemplo, geralmente requer um aumento correspondente no limite de produtividade especificado para o volume.

O *Adaptive QoS* dimensiona automaticamente o valor do grupo de políticas para o tamanho do workload, mantendo a taxa de IOPS para TBs|GBs conforme o tamanho do workload muda. Essa é uma vantagem significativa quando você gerencia centenas ou milhares de workloads em uma implantação grande.

Normalmente, você usa QoS adaptável para ajustar limites máximos de taxa de transferência, mas também pode usá-la para gerenciar andares de taxa de transferência (quando o tamanho do workload aumenta). O tamanho do workload é expresso como o espaço alocado para o objeto de storage ou o espaço usado pelo objeto de storage.

> O espaço usado está disponível para pisos de throughput no ONTAP 9.5 e posterior. Não é suportado para pisos de rendimento no ONTAP 9 .4 e anteriores.

- Uma política *allocated space* mantém a relação IOPS/TB|GB de acordo com o tamanho nominal do objeto de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB terá um limite máximo de taxa de transferência de 15.000 IOPS enquanto o volume permanecer nesse tamanho. Se o volume for redimensionado para 300 GB, a QoS adaptável ajusta o limite da taxa de transferência para 30.000 IOPS.
- Uma política *used space* (o padrão) mantém a taxa IOPS/TB|GB de acordo com a quantidade de dados reais armazenados antes da eficiência de armazenamento. Se a taxa for de 100 IOPS/GB, um volume de 150 GB que tenha 100 GB de dados armazenados teria um limite máximo de taxa de transferência de 10.000 IOPS. À medida que a quantidade de espaço usado muda, a QoS adaptável ajusta o teto de taxa

de transferência de acordo com a taxa.

A partir do ONTAP 9.5, você pode especificar um tamanho de bloco de e/S para o aplicativo que permite que um limite de taxa de transferência seja expresso em IOPS e Mbps. O limite de Mbps é calculado a partir do tamanho do bloco multiplicado pelo limite de IOPS. Por exemplo, um tamanho de bloco de e/S de 32K MB para um limite de IOPS de 6144IOPS GB/TB produz um limite de Mbps de 192MBps GB.

Você pode esperar o seguinte comportamento para tetos e pisos de rendimento:

- Quando um workload é atribuído a um grupo de políticas de QoS adaptável, o teto ou o piso é atualizado imediatamente.
- Quando um workload em um grupo de políticas de QoS adaptável é redimensionado, o teto ou o piso é atualizado em aproximadamente cinco minutos.

A taxa de transferência deve aumentar em pelo menos 10 IOPS antes que as atualizações ocorram.

Grupos de políticas de QoS adaptáveis sempre não são compartilhados: O limite ou o piso da taxa de transferência definida se aplica a cada workload de membro individualmente.

A partir do ONTAP 9.6, os andares de taxa de transferência são suportados no ONTAP Select premium com SSD.

Modelo de grupo de políticas adaptável

A partir do ONTAP 9.13,1, você pode definir um modelo de QoS adaptável em um SVM. Os modelos de grupo de políticas adaptáveis permitem definir andares e tetos de taxa de transferência para todos os volumes em uma SVM.

Os modelos de grupo de políticas adaptáveis só podem ser definidos após a criação do SVM. Use o `vserver modify` comando com o `-qos-adaptive-policy-group-template` parâmetro para definir a política.

Quando você define um modelo de grupo de políticas adaptativas, os volumes criados ou migrados após a configuração da diretiva herdam automaticamente a política. Quaisquer volumes existentes no SVM não serão afetados quando você atribuir o modelo de política. Se você desativar a política no SVM, qualquer volume posteriormente migrado ou criado no SVM não receberá a política. A desativação do modelo de grupo de políticas adaptativas não afeta os volumes que herdaram o modelo de política à medida que retêm o modelo de política.

Para obter mais informações, Defina um modelo de grupo de políticas adaptávelconsulte .

Suporte geral

A tabela a seguir mostra as diferenças no suporte para limites máximos de taxa de transferência, andares de taxa de transferência e QoS adaptável.

Recurso ou recurso	Teto com taxa de transferência	Piso de taxa de transferência	Piso de taxa de transferência v2	QoS adaptável
Versão ONTAP 9	Tudo	9,2 e mais tarde	9,7 e mais tarde	9,3 e mais tarde

Recurso ou recurso	Teto com taxa de transferência	Piso de taxa de transferência	Piso de taxa de transferência v2	QoS adaptável
Plataformas	Tudo	• AFF • C190 * • ONTAP Select premium com SSD *	• AFF • C190 • ONTAP Select premium com SSD	Tudo
Protocolos	Tudo	Tudo	Tudo	Tudo
FabricPool	Sim	Sim, se a política de disposição em categorias estiver definida como "nenhum" e não houver blocos na nuvem.	Sim, se a política de disposição em categorias estiver definida como "nenhum" e não houver blocos na nuvem.	Não
SnapMirror síncrono	Sim	Não	Não	Sim

O suporte ao C190 e ao ONTAP Select começou com o lançamento do ONTAP 9.6.

Workloads compatíveis com limites máximos de taxa de transferência

A tabela a seguir mostra o suporte do workload para limites máximos de taxa de transferência pela versão do ONTAP 9. Volumes raiz, espelhos de compartilhamento de carga e espelhos de proteção de dados não são compatíveis.

Suporte à carga de trabalho - limite máximo	ONTAP 9,0	ONTAP 9,1	ONTAP 9,2	ONTAP 9,3	ONTAP 9.4 - 9,7	ONTAP 9 F.8 e mais tarde
Volume	sim	sim	sim	sim	sim	sim
Ficheiro	sim	sim	sim	sim	sim	sim
LUN	sim	sim	sim	sim	sim	sim
SVM	sim	sim	sim	sim	sim	sim
Volume FlexGroup	não	não	não	sim	sim	sim
qtrees*	não	não	não	não	não	sim

Suporte à carga de trabalho - limite máximo	ONTAP 9,0	ONTAP 9,1	ONTAP 9,2	ONTAP 9,3	ONTAP 9.4 - 9,7	ONTAP 9 F.8 e mais tarde
Vários workloads por grupo de políticas	sim	sim	sim	sim	sim	sim
Grupos de políticas não compartilhados	não	não	não	não	sim	sim

A partir do ONTAP 9.8, o acesso NFS é compatível com qtrees nos volumes FlexVol e FlexGroup com NFS habilitado. A partir do ONTAP 9.9,1, o acesso SMB também é suportado em qtrees nos volumes FlexVol e FlexGroup com SMB ativado.

Workloads compatíveis em pisos de taxa de transferência

A tabela a seguir mostra o suporte do workload para andares de taxa de transferência pela versão do ONTAP 9. Volumes raiz, espelhos de compartilhamento de carga e espelhos de proteção de dados não são compatíveis.

Suporte de carga de trabalho - básico	ONTAP 9,2	ONTAP 9,3	ONTAP 9.4 - 9,7	ONTAP 9.8 - 9.13.0	ONTAP 9.13,1 e posterior
Volume	sim	sim	sim	sim	sim
Ficheiro	não	sim	sim	sim	sim
LUN	sim	sim	sim	sim	sim
SVM	não	não	não	não	sim
Volume FlexGroup	não	não	sim	sim	sim
qtrees *	não	não	não	sim	sim
Vários workloads por grupo de políticas	não	não	sim	sim	sim
Grupos de políticas não compartilhados	não	não	sim	sim	sim

A partir do ONTAP 9.8, o acesso NFS é suportado em qtrees nos volumes FlexVol e FlexGroup com NFS ativado. A partir do ONTAP 9.9,1, o acesso SMB também é suportado em qtrees nos volumes FlexVol e FlexGroup com SMB ativado.

Workloads compatíveis com QoS adaptável

A tabela a seguir mostra o suporte do workload para QoS adaptável pela versão do ONTAP 9. Volumes raiz, espelhos de compartilhamento de carga e espelhos de proteção de dados não são compatíveis.

Suporte a workload - QoS adaptável	ONTAP 9,3	ONTAP 9.4 - 9.13.0	ONTAP 9.13,1 e posterior
Volume	sim	sim	sim
Ficheiro	não	sim	sim
LUN	não	sim	sim
SVM	não	não	sim
Volume FlexGroup	não	sim	sim
Vários workloads por grupo de políticas	sim	sim	sim
Grupos de políticas não compartilhados	sim	sim	sim

Número máximo de cargas de trabalho e grupos de políticas

A tabela a seguir mostra o número máximo de cargas de trabalho e grupos de políticas por versão do ONTAP 9.

Suporte a workload	ONTAP 9 .3 e anteriores	ONTAP 9 .4 e mais tarde
Máximo de workloads por cluster	12.000	40.000
Máximo de workloads por nó	12.000	40.000
Máximo de grupos de políticas	12.000	12.000

Ativar ou desativar os pisos de rendimento v2

Você pode ativar ou desativar os andares de taxa de transferência v2 no AFF. A predefinição é Enabled (activado). Com os andares v2 ativados, os andares de taxa de transferência podem ser atendidos quando os controladores são muito usados em detrimento da latência mais alta em outros workloads. Os pisos v2 aplicam-se a QoS e QoS adaptável.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Introduza um dos seguintes comandos:

Se você quiser…	Use este comando:
Desativar pisos v2	`qos settings throughput-floors-v2 -enable false`
Ativar os pisos v2	`qos settings throughput-floors-v2 -enable true`

Para desativar os pisos de taxa de transferência v2 num cluster MetroCluster, tem de executar o.

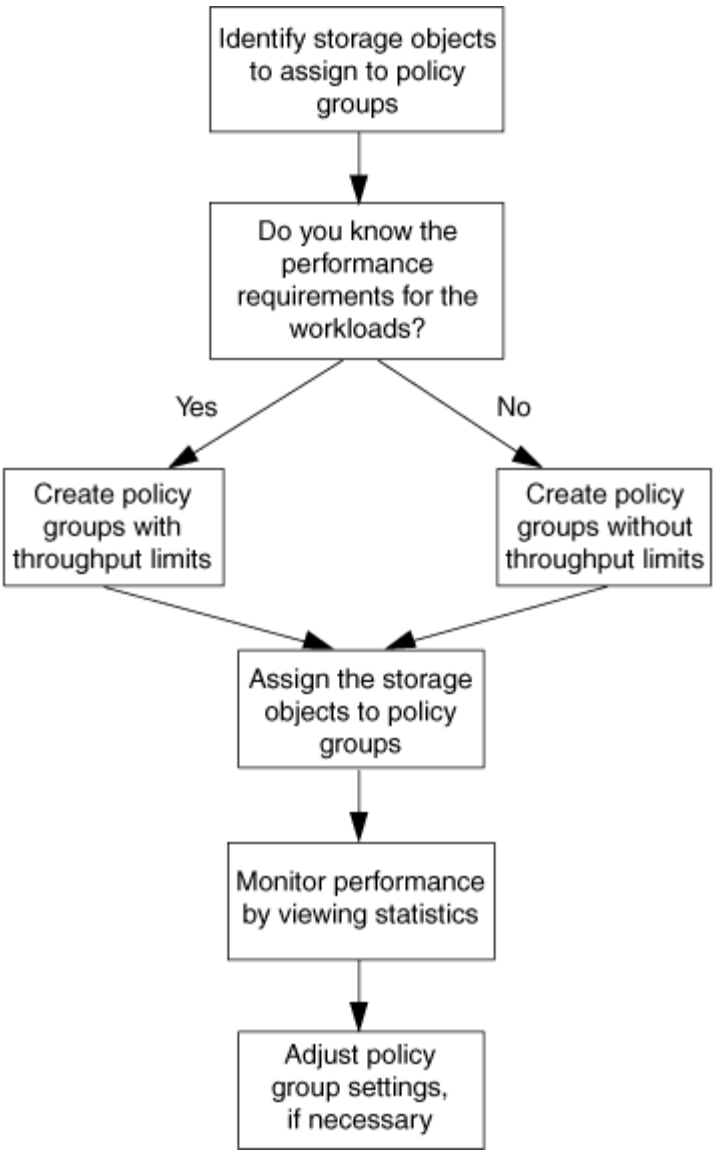
`qos settings throughput-floors-v2 -enable false`

comando nos clusters de origem e destino.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

Fluxo de trabalho de QoS do storage

Se você já conhece os requisitos de desempenho para os workloads que deseja gerenciar com QoS, poderá especificar o limite de taxa de transferência ao criar o grupo de políticas. Caso contrário, você pode esperar até que você monitore as cargas de trabalho para especificar o limite.



Defina um limite de taxa de transferência com QoS

Você pode usar o `max-throughput` campo de um grupo de políticas para definir um limite máximo de taxa de transferência para workloads de objetos de storage (QoS Max). Você pode aplicar o grupo de políticas ao criar ou modificar o objeto de armazenamento.

O que você vai precisar

- Você deve ser um administrador de cluster para criar um grupo de políticas.
- Você deve ser um administrador de cluster para aplicar um grupo de políticas a um SVM.

Sobre esta tarefa

- A partir do ONTAP 9.4, você pode usar um grupo de políticas de QoS *não compartilhado* para especificar que o limite de taxa de transferência definido se aplica a cada workload de membro individualmente. Caso contrário, o grupo de políticas é *compartilhado:* a taxa de transferência total para as cargas de trabalho atribuídas ao grupo de políticas não pode exceder o limite máximo especificado.

  Defina `-is-shared=false` para que o `qos policy-group create` comando especifique um grupo de políticas não compartilhado.

- Você pode especificar o limite de taxa de transferência para o limite máximo em IOPS, MB/s ou IOPS, MB/s. Se você especificar IOPS e MB/s, qualquer limite atingido primeiro será aplicado.

> Se você definir um teto e um piso para a mesma carga de trabalho, poderá especificar o limite de taxa de transferência para o limite máximo apenas em IOPS.

- Um objeto de storage que esteja sujeito a um limite de QoS precisa estar contido pelo SVM a que o grupo de políticas pertence. Vários grupos de políticas podem pertencer ao mesmo SVM.
- Não é possível atribuir um objeto de armazenamento a um grupo de políticas se o objeto que contém ou os objetos filho pertencerem ao grupo de políticas.
- É uma prática recomendada de QoS aplicar um grupo de políticas ao mesmo tipo de objetos de storage.

Passos

1. Criar um grupo de políticas:

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   Para obter a sintaxe completa do comando, consulte a página man. Você pode usar o `qos policy-group modify` comando para ajustar os tetos de taxa de transferência.

   O comando a seguir cria o grupo de políticas compartilhadas `pg-vs1` com uma taxa de transferência máxima de 5.000 IOPS:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   O comando a seguir cria o grupo de políticas não compartilhadas `pg-vs3` com uma taxa de transferência máxima de 100 IOPS e 400 Kb/S:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   O comando a seguir cria o grupo de políticas não compartilhadas `pg-vs4` sem um limite de taxa de transferência:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. Aplique um grupo de políticas a um SVM, arquivo, volume ou LUN:

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   Para obter a sintaxe completa do comando, consulte as páginas man. Você pode usar o *`storage_object`* `modify` comando para aplicar um grupo de políticas diferente ao objeto de armazenamento.

O comando a seguir aplica o grupo de políticas `pg-vs1` ao SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Os comandos a seguir aplicam o grupo de políticas `pg-app` aos volumes `app1` e `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. Monitorar o desempenho do grupo de políticas:

   `qos statistics performance show`

   Para obter a sintaxe completa do comando, consulte a página man.

   Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

   O comando a seguir mostra o desempenho do grupo de políticas:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. Monitorar a performance do workload:

   `qos statistics workload performance show`

   Para obter a sintaxe completa do comando, consulte a página man.

   Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

   O comando a seguir mostra o desempenho da carga de trabalho:

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-               -    12320        47.84MB/s  1215.00us
app1-wid7967       7967     7219        28.20MB/s   319.00us
vs1-wid12279      12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS      14       55        10.92KB/s   236.00us
_Scan_Backgro..    5688       20            0KB/s        0ms
```

Use o `qos statistics workload latency show` comando para visualizar estatísticas detalhadas de latência para workloads de QoS.

Defina um piso de taxa de transferência com QoS

Você pode usar o `min-throughput` campo de um grupo de políticas para definir um piso de taxa de transferência para workloads de objetos de storage (QoS min). Você pode aplicar o grupo de políticas ao criar ou modificar o objeto de armazenamento. A partir do ONTAP 9.8, você pode especificar o piso da taxa de transferência em IOPS ou Mbps, ou IOPS e Mbps.

Antes de começar

- Você deve estar executando o ONTAP 9.2 ou posterior. Os pisos de taxa de transferência estão disponíveis a partir do ONTAP 9.2.
- Você deve ser um administrador de cluster para criar um grupo de políticas.
- A partir do ONTAP 9.13,1, você pode aplicar pisos de taxa de transferência no nível SVM usando um modelo de grupo de políticas adaptável. Não é possível definir um modelo de grupo de políticas adaptável em um SVM com um grupo de políticas de QoS.

Sobre esta tarefa

- A partir do ONTAP 9.4, você pode usar um grupo de políticas de QoS *não compartilhado* para especificar que o piso da taxa de transferência definido seja aplicado individualmente a cada workload de membro. Essa é a única condição em que um grupo de políticas para uma área de transferência pode ser aplicado a várias cargas de trabalho.

  Defina `-is-shared=false` para que o `qos policy-group create` comando especifique um grupo de políticas não compartilhado.

- A taxa de transferência para uma carga de trabalho pode ficar abaixo do nível especificado se houver capacidade de desempenho (espaço livre) insuficiente no nó ou no agregado.
- Um objeto de storage que esteja sujeito a um limite de QoS precisa estar contido pelo SVM a que o grupo de políticas pertence. Vários grupos de políticas podem pertencer ao mesmo SVM.
- É uma prática recomendada de QoS aplicar um grupo de políticas ao mesmo tipo de objetos de storage.
- Um grupo de políticas que define um piso de taxa de transferência não pode ser aplicado a um SVM.

Passos

1. Verifique se há capacidade de desempenho adequada no nó ou no agregado, conforme descrito

"Identificação da capacidade de performance restante"em .

2. Criar um grupo de políticas:

   `qos policy-group create -policy group policy_group -vserver SVM -min -throughput qos_target -is-shared true|false`

   Para obter a sintaxe de comando completa, consulte a página man para sua versão do ONTAP. Você pode usar o `qos policy-group modify` comando para ajustar os andares de taxa de transferência.

   O comando a seguir cria o grupo de políticas compartilhadas `pg-vs2` com uma taxa de transferência mínima de 1.000 IOPS:

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   O comando a seguir cria o grupo de políticas não compartilhadas `pg-vs4` sem um limite de taxa de transferência:

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

3. Aplicar um grupo de políticas a um volume ou LUN:

   storage_object `create -vserver` *SVM* `-qos-policy-group` *policy_group*

   Para obter a sintaxe completa do comando, consulte as páginas man. Você pode usar o `_storage_object_modify` comando para aplicar um grupo de políticas diferente ao objeto de armazenamento.

   O comando a seguir aplica o grupo de políticas `pg-app2` ao volume `app2`:

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

4. Monitorar o desempenho do grupo de políticas:

   `qos statistics performance show`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

   O comando a seguir mostra o desempenho do grupo de políticas:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. Monitorar a performance do workload:

   `qos statistics workload performance show`

   Para obter a sintaxe completa do comando, consulte a página man.

   > Monitore o desempenho do cluster. Não use uma ferramenta no host para monitorar o desempenho.

   O comando a seguir mostra o desempenho da carga de trabalho:

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

   > Use o `qos statistics workload latency show` comando para visualizar estatísticas detalhadas de latência para workloads de QoS.

Use grupos de políticas de QoS adaptáveis

Você pode usar um grupo de políticas *Adaptive QoS* para escalar automaticamente um limite de taxa de transferência ou um tamanho de chão para volume, mantendo a taxa de IOPS para TBs|GBs conforme o tamanho do volume muda. Essa é uma vantagem significativa quando você gerencia centenas ou milhares de workloads em uma implantação grande.

Antes de começar

- Você deve estar executando o ONTAP 9.3 ou posterior. Os grupos de políticas de QoS adaptáveis estão disponíveis a partir do ONTAP 9.3.
- Você deve ser um administrador de cluster para criar um grupo de políticas.

Sobre esta tarefa

Um objeto de storage pode ser membro de um grupo de políticas adaptáveis ou de um grupo de políticas não adaptáveis, mas não ambos. O SVM do objeto de storage e a política devem ser os mesmos. O objeto de storage deve estar on-line.

Grupos de políticas de QoS adaptáveis sempre não são compartilhados: O limite ou o piso da taxa de transferência definida se aplica a cada workload de membro individualmente.

A proporção de limites de taxa de transferência para o tamanho do objeto de armazenamento é determinada pela interação dos seguintes campos:

- `expected-iops` É o mínimo esperado de IOPS por TB|GB alocado.

> `expected-iops` É garantido apenas nas plataformas AFF. `expected-iops` Será garantido para o FabricPool somente se a política de disposição em categorias estiver definida como "nenhuma" e não houver blocos na nuvem. `expected-iops` É garantido para volumes que não estão em uma relação síncrona SnapMirror.

- `peak-iops` É o máximo de IOPS possível por TB|GB alocado ou usado.
- `expected-iops-allocation` especifica se o espaço alocado (o padrão) ou o espaço usado é usado para iops-esperado.

> `expected-iops-allocation` Está disponível no ONTAP 9.5 e posterior. Ele não é suportado no ONTAP 9.4 e anterior.

- `peak-iops-allocation` especifica se o espaço alocado ou o espaço usado (o padrão) é usado para `peak-iops`.
- `absolute-min-iops` É o número mínimo absoluto de IOPS. Você pode usar este campo com objetos de armazenamento muito pequenos. Substitui ambos `peak-iops` e/ `expected-iops`ou quando `absolute-min-iops` é maior do que o `expected-iops` calculado .

  Por exemplo, se você definir `expected-iops` como 1.000 IOPS/TB e o tamanho do volume for inferior a 1 GB, o calculado `expected-iops` será uma IOP fracionária. O calculado `peak-iops` será uma fração ainda menor. Você pode evitar isso definindo `absolute-min-iops` um valor realista.

- `block-size` Especifica o tamanho do bloco de e/S da aplicação. A predefinição é 32K. Os valores válidos são 8K, 16K, 32K, 64K, QUALQUER. QUALQUER significa que o tamanho do bloco não é imposto.

Três grupos de políticas de QoS adaptáveis padrão estão disponíveis, como mostrado na tabela a seguir. Você pode aplicar esses grupos de políticas diretamente a um volume.

Grupo de políticas padrão	IOPS/TB esperados	IOPS/TB de pico	IOPS mín. Absoluto
`extreme`	6.144	12.288	1000

`performance`	2.048	4.096	500
`value`	128	512	75

Não é possível atribuir um objeto de armazenamento a um grupo de políticas se o objeto que contém ou os objetos filho pertencerem a um grupo de políticas. A tabela a seguir lista as restrições.

Se você atribuir…	**Então você não pode atribuir…**
SVM em um grupo de políticas	Quaisquer objetos de storage contidos pelo SVM em um grupo de políticas
Volume para um grupo de políticas	Volume contendo SVM ou LUNs filho, em um grupo de políticas
LUN para um grupo de políticas	LUN que contêm volume ou SVM em um grupo de políticas
Arquivo para um grupo de políticas	Os arquivos contêm volume ou SVM em um grupo de políticas

Passos

1. Criar um grupo de políticas de QoS adaptável:

   `qos adaptive-policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-expected-iops` *`number_of_iops`*`/TB|GB -peak-iops` *`number_of_iops`*`/TB|GB -expected -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-space -absolute-min-iops` *`number_of_iops`* `-block-size 8K|16K|32K|64K|ANY`

   Para obter a sintaxe completa do comando, consulte a página man.

   > `-expected-iops-allocation` E `-block-size` está disponível em ONTAP 9.5 e posterior. Essas opções não são suportadas no ONTAP 9.4 e versões anteriores.

   O comando a seguir cria um grupo de políticas de QoS adaptável `adpg-app1` `-expected-iops` definido como 300 IOPS/TB, `-peak-iops` definido como 1.000 IOPS/TB, `-peak-iops-allocation` definido como `used-space`e `-absolute-min-iops` definido como 50 IOPS:

   ```
   cluster1::> qos adaptive-policy-group create -policy group adpg-app1
   -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
   -allocation used-space -absolute-min-iops 50iops
   ```

2. Aplicar um grupo de políticas de QoS adaptável a um volume:

   `volume create -vserver SVM -volume` *`volume`* `-aggregate` *`aggregate`* `-size` *`number_of`* `TB|GB -qos-adaptive-policy-group` *`policy_group`*

Para obter a sintaxe completa do comando, consulte as páginas man.

O comando a seguir aplica o grupo de políticas de QoS adaptável `adpg-app1` ao volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Os comandos a seguir aplicam o grupo de políticas de QoS adaptável padrão `extreme` ao novo volume `app4` e ao volume existente `app5` . O limite máximo de taxa de transferência definido para o grupo de políticas aplica-se a volumes `app4` e `app5` individualmente:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

Defina um modelo de grupo de políticas adaptável

A partir do ONTAP 9.13,1, você pode aplicar pisos e tetos de taxa de transferência no nível SVM usando um modelo de grupo de políticas adaptável.

Sobre esta tarefa

- O modelo de grupo de políticas adaptativas é uma política `apg1`padrão . A política pode ser modificada a qualquer momento. Ela só pode ser definida com a API REST CLI ou ONTAP e só pode ser aplicada a SVMs existentes.
- O modelo de grupo de políticas adaptável afeta apenas os volumes criados ou migrados para o SVM após você definir a política. Os volumes existentes no SVM mantêm seu status atual.

  Se você desabilitar o modelo de grupo de políticas adaptáveis, os volumes no SVM manterão suas políticas existentes. Somente os volumes posteriormente criados ou migrados para o SVM serão afetados pelo desfalecimento.

- Não é possível definir um modelo de grupo de políticas adaptável em um SVM com um grupo de políticas de QoS.
- Os modelos de grupo de políticas adaptáveis são projetados para plataformas AFF. Um modelo de grupo de políticas adaptável pode ser definido em outras plataformas, mas a política pode não impor uma taxa de transferência mínima. Da mesma forma, você pode adicionar um modelo de grupo de políticas adaptável a um SVM em um agregado do FabricPool ou em um agregado que não ofereça suporte a taxa de transferência mínima. No entanto, o nível de taxa de transferência não será imposto.
- Se o SVM estiver em uma configuração do MetroCluster ou em uma relação do SnapMirror, o modelo de grupo de políticas adaptável será aplicado no SVM espelhado.

Passos

1. Modifique o SVM para aplicar o modelo de grupo de políticas adaptável:
   `vserver modify -qos-adaptive-policy-group-template apg1`

2. Confirme se a política foi definida:
   `vserver show -fields qos-adaptive-policy-group`

Monitore o desempenho do cluster com o Unified Manager

Com o Active IQ Unified Manager, você pode maximizar a disponibilidade e manter o controle da infraestrutura de storage NetApp AFF e FAS para aumentar a escalabilidade, a capacidade de suporte, a performance e a segurança.

O Active IQ Unified Manager monitora continuamente a integridade do sistema e envia alertas para que sua organização possa liberar recursos da equipe DE TI. Você pode visualizar instantaneamente o status do storage em um único painel e solucionar problemas rapidamente por meio das ações recomendadas.

O gerenciamento de dados é simplificado porque é possível descobrir, monitorar e receber notificações para gerenciar proativamente o storage e resolver problemas com rapidez. A eficiência dos administradores é aprimorada porque é possível monitorar petabytes de dados em um único dashboard e gerenciar os dados em escala.

Com o Active IQ Unified Manager, você pode acompanhar as flutuações das demandas de negócios, otimizando o desempenho usando dados de desempenho e análises avançadas. Os recursos de relatórios permitem que você acesse relatórios padrão ou crie relatórios operacionais personalizados para atender às necessidades específicas de sua empresa.

Links relacionados:

- "Saiba mais sobre o Active IQ Unified Manager"
- "Comece a usar o Active IQ Unified Manager para VMware"
- "Comece a usar o Active IQ Unified Manager para Linus"
- "Comece a usar o Active IQ Unified Manager para Windows"

Monitore o desempenho do cluster com o Cloud Insights

O NetApp Cloud Insights é uma ferramenta de monitoramento que oferece visibilidade de toda a sua infraestrutura. Com o Cloud Insights, você pode monitorar, solucionar problemas e otimizar todos os recursos, incluindo suas nuvens públicas e seus data centers privados.

Cloud Insights vem em duas edições

A edição básica do Cloud Insights foi projetada especificamente para monitorar e otimizar seus ativos do NetApp Data Fabric. Ele fornece análises avançadas para conexões entre todos os recursos do NetApp, incluindo HCI e All Flash FAS (AFF) no ambiente gratuitamente.

O Cloud Insights Standard Edition se concentra não apenas em componentes de infraestrutura habilitados para NetApp Data Fabric, mas também em ambientes de vários fornecedores e multicloud. Com seus recursos enriquecidos, você pode acessar o suporte para mais de 100 serviços e recursos.

No mundo de hoje, com recursos em jogo de seus data centers no local para várias nuvens públicas, é crucial ter a visão completa, desde a própria aplicação até o disco de back-end do storage array. O suporte adicional para monitoramento de aplicativos (como Kafka, MongoDB e nginx) fornece as informações e o conhecimento

que você precisa para operar no nível ideal de utilização, bem como com o buffer de risco perfeito.

Ambas as edições (Basic e Standard) podem se integrar ao NetApp Active IQ Unified Manager. Os clientes que usam o Active IQ Unified Manager podem ver as informações de associação dentro da interface de usuário do Cloud Insights. As notificações postadas no Active IQ Unified Manager não são negligenciadas e podem ser correlacionadas a eventos no Cloud Insights. Em outras palavras, você obtém o melhor dos dois mundos.

Monitore, solucione problemas e otimize todos os seus recursos

O Cloud Insights ajuda você a reduzir significativamente o tempo para resolver problemas e evitar que eles afetem os usuários finais. Ele também ajuda a reduzir os custos de infraestrutura de nuvem. Sua exposição a ameaças internas é reduzida ao proteger seus dados com inteligência acionável.

O Cloud Insights oferece visibilidade de toda a sua infraestrutura híbrida em um só lugar, da nuvem pública ao data center. Você pode criar instantaneamente painéis relevantes que podem ser personalizados de acordo com suas necessidades específicas. Você também pode criar alertas direcionados e condicionais que sejam específicos e relevantes para as necessidades da sua organização.

A detecção avançada de anomalias ajuda a corrigir problemas de forma proativa, antes que eles ocorram. Você pode visualizar a contenção e a degradação de recursos automaticamente para restaurar os workloads afetados com rapidez. A solução de problemas vai mais rapidamente com a hierarquia de relações criada automaticamente entre os diferentes componentes da pilha.

Você pode identificar recursos não utilizados ou abandonados em todo o seu ambiente, o que ajuda a descobrir oportunidades de dimensionar corretamente a infraestrutura e otimizar todo o seu gasto.

O Cloud Insights visualiza a topologia do sistema para entender a arquitetura do Kubernetes. Você pode monitorar a integridade dos clusters do Kubernetes, incluindo os nós com problemas, e aumentar o zoom quando encontrar um problema.

O Cloud Insights ajuda você a proteger os dados organizacionais contra a utilização indevida por usuários mal-intencionados ou comprometidos por meio de aprendizado de máquina avançado e detecção de anomalias. Isso proporciona informações úteis sobre ameaças internas.

O Cloud Insights ajuda você a visualizar métricas do Kubernetes para que você possa entender completamente as relações entre seus pods, nós e clusters. Você pode avaliar a integridade de um cluster ou um pod de trabalho, bem como a carga que ele está processando atualmente, permitindo que você assuma o comando do cluster K8S e controle a integridade e o custo da implantação.

Links relacionados

- "Saiba mais sobre o Cloud Insights"
- "Comece a usar o Cloud Insights"

Log de auditoria

Como o ONTAP implementa o log de auditoria

As atividades de gerenciamento registradas no log de auditoria são incluídas nos relatórios padrão do AutoSupport e certas atividades de Registro são incluídas nas mensagens do EMS. Você também pode encaminhar o log de auditoria para destinos especificados e exibir arquivos de log de auditoria usando a CLI ou um navegador da

Web.

A partir do ONTAP 9.11,1, você pode exibir o conteúdo do log de auditoria usando o Gerenciador do sistema.

A partir do ONTAP 9.12,1, o ONTAP fornece alertas de adulteração para logs de auditoria. O ONTAP executa um trabalho de segundo plano diário para verificar se há adulteração de arquivos audit.log e envia um alerta EMS se ele encontrar arquivos de log que foram alterados ou adulterados.

O ONTAP Registra as atividades de gerenciamento que são executadas no cluster, por exemplo, qual solicitação foi emitida, o usuário que acionou a solicitação, o método de acesso do usuário e a hora da solicitação.

As atividades de gestão podem ser um dos seguintes tipos:

- Definir solicitações, que normalmente se aplicam a comandos ou operações que não sejam exibidas:
  - Essas solicitações são emitidas quando você executa um `create` comando , `modify`, ou `delete`, por exemplo.
  - As solicitações de conjunto são registradas por padrão.
- OBTENHA solicitações, que recuperam informações e exibem na interface de gerenciamento:
  - Essas solicitações são emitidas quando você executa um `show` comando, por exemplo.
  - As SOLICITAÇÕES GET não são registradas por padrão, mas você pode controlar se as solicitações GET enviadas da CLI do ONTAP (`-cliget`), da API do ONTAP (`-ontapiget`) ou da API REST (`-httpget`) estão registradas no arquivo.

O ONTAP Registra atividades de gerenciamento `/mroot/etc/log/mlog/audit.log` no arquivo de um nó. Comandos dos três shells para comandos CLI - o clustershell, o nodeshell e o systemshell não interativo (comandos do systemshell interativo não são registrados) - assim como os comandos API são registrados aqui. Os logs de auditoria incluem carimbos de data/hora para mostrar se todos os nós de um cluster estão sincronizados com a hora.

O `audit.log` arquivo é enviado pela ferramenta AutoSupport para os destinatários especificados. Você também pode encaminhar o conteúdo de forma segura para destinos externos especificados por você; por exemplo, um Splunk ou um servidor syslog.

O `audit.log` arquivo é girado diariamente. A rotação também ocorre quando atinge 100 MB de tamanho, e as 48 cópias anteriores são preservadas (com um total máximo de 49 arquivos). Quando o arquivo de auditoria executa sua rotação diária, nenhuma mensagem EMS é gerada. Se o arquivo de auditoria girar porque seu limite de tamanho de arquivo é excedido, uma mensagem EMS é gerada.

Alterações ao registo de auditoria no ONTAP 9

A partir do ONTAP 9, o `command-history.log` arquivo é substituído pelo `audit.log`, e o `mgwd.log` arquivo não contém mais informações de auditoria. Se você estiver atualizando para o ONTAP 9, revise todos os scripts ou ferramentas que se referem aos arquivos legados e seus conteúdos.

Após a atualização para o ONTAP 9, os arquivos existentes `command-history.log` são preservados. Eles são girados para fora (excluídos) à medida que novos `audit.log` arquivos são girados em (criados).

Ferramentas e scripts que verificam o `command-history.log` arquivo podem continuar funcionando, porque

um link de software de `command-history.log` para `audit.log` é criado na atualização. No entanto, ferramentas e scripts que verificam o `mgwd.log` arquivo falharão, porque esse arquivo não contém mais informações de auditoria.

Além disso, os logs de auditoria no ONTAP 9 e posterior não incluem mais as seguintes entradas porque não são consideradas úteis e causam atividade de Registro desnecessária:

- Comandos internos executados pelo ONTAP (ou seja, onde o nome de usuário é root)
- Aliases de comando (separadamente do comando para o qual eles apontam)

A partir do ONTAP 9, você pode transmitir os logs de auditoria de forma segura para destinos externos usando os protocolos TCP e TLS.

Exibir conteúdo do log de auditoria

Você pode exibir o conteúdo dos arquivos do cluster `/mroot/etc/log/mlog/audit.log` usando a CLI do ONTAP, o Gerenciador de sistema ou um navegador da Web.

As entradas do arquivo de log do cluster incluem o seguinte:

Tempo
O carimbo de data/hora da entrada de registo.

Aplicação
A aplicação utilizada para ligar ao cluster. Exemplos de valores possíveis são `internal`, `console`, `ssh`, `http`, , , `ontapi`, `snmp` `rsh`, , , `telnet` e `service-processor`.

Utilizador
O nome de utilizador do utilizador remoto.

Estado
O estado atual da solicitação de auditoria, que pode ser `success`, `pending` ou `error`.

Mensagem
Um campo opcional que pode conter erro ou informações adicionais sobre o status de um comando.

Session ID
O Session ID no qual o pedido é recebido. Cada SSH *session* recebe um Session ID, enquanto cada HTTP, ONTAPI ou SNMP *Request* recebe um Session ID exclusivo.

Armazenamento VM
O SVM por meio do qual o usuário se conectou.

Âmbito de aplicação
É exibido `svm` quando a solicitação está em uma VM de armazenamento de dados; caso contrário, exibe `cluster`.

ID do comando
O ID de cada comando recebido em uma sessão CLI. Isso permite correlacionar uma solicitação e uma resposta. As solicitações ZAPI, HTTP e SNMP não têm IDs de comando.

Você pode exibir as entradas de log do cluster a partir da CLI do ONTAP, de um navegador da Web e, começando com ONTAP 9.11,1, do Gerenciador do sistema.

System Manager

- Para exibir o inventário, selecione **Eventos e trabalhos > Logs de auditoria**. Cada coluna tem controles para filtrar, classificar, pesquisar, mostrar e categorias de inventário. Os detalhes do inventário podem ser baixados como uma pasta de trabalho do Excel.
- Para definir filtros, clique no botão **filtro** no canto superior direito e selecione os campos desejados. Você também pode visualizar todos os comandos executados na sessão em que ocorreu uma falha clicando no link Session ID.

CLI

Para exibir entradas de auditoria mescladas de vários nós no cluster, digite `security audit log show <[parameters]>`

Você pode usar o `security audit log show` comando para exibir entradas de auditoria para nós individuais ou mesclados de vários nós no cluster. Você também pode exibir o conteúdo do `/mroot/etc/log/mlog` diretório em um único nó usando um navegador da Web. Consulte a página de manual para obter detalhes.

Navegador da Web

Você pode exibir o conteúdo do `/mroot/etc/log/mlog` diretório em um único nó usando um navegador da Web. "Saiba mais sobre como acessar os arquivos de log, despejo de memória e MIB de um nó usando um navegador da Web".

Gerenciar as configurações de solicitação DE auditoria

Embora as SOLICITAÇÕES DE CONJUNTO sejam registradas por padrão, as SOLICITAÇÕES DE OBTENÇÃO não são. No entanto, você pode controlar se as solicitações GET enviadas do ONTAP HTML (`-httpget`), da CLI do ONTAP (`-cliget`) ou das APIs do ONTAP (`-ontapiget`) estão registradas no arquivo.

Você pode modificar as configurações de log de auditoria a partir da CLI do ONTAP e, a partir do ONTAP 9.11,1, do Gerenciador do sistema.

System Manager

1. Selecione **Eventos e trabalhos > Registos de auditoria**.
2. Clique no canto superior direito e escolha as solicitações a serem adicionadas ou removidas.

CLI

- Para especificar que AS SOLICITAÇÕES GET da CLI ou APIs do ONTAP devem ser registradas no log de auditoria (o arquivo audit.log), além das solicitações de conjunto padrão, digite `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Para visualizar as definições atuais, introduza `security audit show`

Consulte as páginas de manual para obter detalhes.

Gerenciar destinos de log de auditoria

Você pode encaminhar o log de auditoria para um máximo de 10 destinos. Por exemplo, você pode encaminhar o log para um servidor Splunk ou syslog para fins de monitoramento, análise ou backup.

Sobre esta tarefa

Para configurar o encaminhamento, você deve fornecer o endereço IP do host syslog ou Splunk, seu número de porta, um protocolo de transmissão e a facilidade syslog para usar nos logs encaminhados. "Saiba mais sobre as instalações do syslog".

Pode selecionar um dos seguintes valores de transmissão utilizando o `-protocol` parâmetro:

UDP não encriptado
: Protocolo de datagrama de usuário sem segurança (padrão)

TCP não criptografado
: Protocolo de controlo da transmissão sem segurança

TCP criptografado
: Protocolo de controle de transmissão com TLS (Transport Layer Security) e opção **Verify Server** está disponível quando o protocolo criptografado TCP é selecionado.

A porta padrão é 514 para UDP e 6514 para TCP, mas você pode designar qualquer porta que atenda às necessidades de sua rede.

Você pode selecionar um dos seguintes formatos de mensagem usando o `-message-format` comando:

legacy-NetApp
: Uma variação do formato RFC-3164 Syslog (formato: <PRIVAL>

rfc-5424
: Formato syslog de acordo com RFC-5424 (formato: <PRIVAL>

Você pode encaminhar logs de auditoria da CLI do ONTAP e, a partir do ONTAP 9.11,1, do Gerenciador de

sistemas.

System Manager

- Para exibir destinos de log de auditoria, selecione **Cluster >Settings**. Uma contagem de destinos de log é mostrada no bloco **Notification Management**. Clique ⋮ para mostrar detalhes.
- Para adicionar, modificar ou eliminar destinos de registo de auditoria, selecione **Eventos e trabalhos > Registos de auditoria** e, em seguida, clique em **gerir destinos de auditoria** no canto superior direito do ecrã. Clique + Add em ou clique ⋮ na coluna **Endereço do host** para editar ou excluir entradas.

CLI

1. Para cada destino para o qual você deseja encaminhar o log de auditoria, especifique o endereço IP de destino ou o nome do host e quaisquer opções de segurança.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

   - Se o `cluster log-forwarding create` comando não puder fazer ping no host de destino para verificar a conetividade, o comando falhará com um erro. Embora não seja recomendado, usar o `-force` parâmetro com o comando ignora a verificação de conetividade.
   - Quando você define o `-verify-server` parâmetro como `true`, a identidade do destino de encaminhamento de log é verificada validando seu certificado. Pode definir o valor `true` apenas quando selecionar o `tcp-encrypted` valor no `-protocol` campo.

2. Verifique se os Registros de destino estão corretos usando o `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show

                                              Verify Syslog
Destination Host          Port   Protocol     Server Facility
------------------------- ------ -------- ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

Consulte a `cluster log-forwarding create` página de manual para obter detalhes.

AutoSupport

Saiba mais sobre o AutoSupport

Sobre o AutoSupport

O AutoSupport é um mecanismo que monitora proativamente a integridade do sistema e envia mensagens automaticamente para o suporte técnico da NetApp, sua organização de suporte interno e um parceiro de suporte. Embora as mensagens do AutoSupport para suporte técnico estejam habilitadas por padrão, você deve definir as opções corretas e ter um host de e-mail válido para que as mensagens sejam enviadas para sua organização interna de suporte.

Somente o administrador do cluster pode executar o gerenciamento do AutoSupport. O administrador da máquina virtual de storage (SVM) não tem acesso ao AutoSupport.

O AutoSupport é ativado por padrão quando você configura o sistema de storage pela primeira vez. O AutoSupport começa a enviar mensagens para o suporte técnico 24 horas após a ativação do AutoSupport. Você pode encurtar o período de 24 horas atualizando ou revertendo o sistema, modificando a configuração do AutoSupport ou alterando o tempo do sistema para ser algo diferente de um período de 24 horas.

> Você pode desativar o AutoSupport a qualquer momento, mas deve deixá-lo habilitado. A ativação do AutoSupport pode ajudar a acelerar significativamente a determinação e a resolução de problemas em caso de problema no sistema de storage. Por padrão, o sistema coleta informações do AutoSupport e as armazena localmente, mesmo que você desative o AutoSupport.

Para obter mais informações sobre o AutoSupport, consulte o site de suporte da NetApp.

Informações relacionadas

- "Suporte à NetApp"
- "Referência do comando ONTAP"

Sobre o consultor digital e o AutoSupport

O componente AutoSupport do ONTAP coleta telemetria e envia-a para análise. O consultor digital analisa os dados do AutoSupport e fornece cuidado e otimização proativos. Usando inteligência artificial, o Digital Advisor pode identificar possíveis problemas e ajudá-lo a resolvê-los antes que eles afetem seu negócio.

O Digital Advisor permite otimizar sua infraestrutura de dados em toda a nuvem híbrida global, fornecendo análises preditivas práticas e suporte proativo por meio de um portal baseado na nuvem e aplicativo móvel. Insights e recomendações orientados por dados do consultor digital estão disponíveis para todos os clientes da NetApp com um contrato de SupportEdge ativo (os recursos variam de acordo com o produto e a camada de suporte).

Aqui estão algumas coisas que você pode fazer com o Digital Advisor:

- Planejar atualizações. O consultor digital identifica problemas no seu ambiente que podem ser resolvidos ao atualizar para uma versão mais recente do ONTAP e o componente do consultor de atualização ajuda

você a Planejar uma atualização bem-sucedida.

- Veja o bem-estar do sistema. Seu painel do Digital Advisor relata quaisquer problemas de bem-estar e ajuda você a corrigir esses problemas. Monitore a capacidade do sistema para garantir que você nunca fique sem espaço de armazenamento. Veja casos de suporte para o seu sistema.
- Gerenciar a performance. O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no System Manager. Identifique problemas de configuração e sistema que estejam afetando a performance.
- Maximizar a eficiência: Visualize as métricas de eficiência de storage e identifique maneiras de armazenar mais dados em menos espaço.
- Ver inventário e configuração. O Digital Advisor exibe o inventário completo e as informações de configuração de software e hardware. Veja quando os contratos de serviço estão expirando e renove-os para garantir que você permaneça suportado.

Informações relacionadas

"Documentação do NetApp: Consultor digital"

"Inicie o Digital Advisor"

"Serviços da SupportEdge"

Quando e onde as mensagens AutoSupport são enviadas

O AutoSupport envia mensagens para diferentes destinatários, dependendo do tipo de mensagem. Aprender quando e onde o AutoSupport envia mensagens pode ajudá-lo a entender as mensagens que você recebe por e-mail ou exibição no site do consultor digital.

Salvo especificação em contrário, as configurações nas tabelas a seguir são parâmetros do `system node autosupport modify` comando.

Mensagens acionadas por eventos

Quando ocorrem eventos no sistema que exigem ação corretiva, o AutoSupport envia automaticamente uma mensagem acionada por evento.

Quando a mensagem é enviada	Onde a mensagem é enviada
O AutoSupport responde a um evento de ativação no EMS	Endereços especificados em `-to` e `-noteto`. (Apenas eventos críticos que afetam o serviço são enviados.) Endereços especificados em `-partner-address` Suporte técnico, se `-support` estiver definido como `enable`

Mensagens agendadas

O AutoSupport envia automaticamente várias mensagens em um horário regular.

Quando a mensagem é enviada	Onde a mensagem é enviada
Diariamente (por padrão, enviado entre as 12:00h e as 1:00h como uma mensagem de log)	Endereços especificados em `-partner-address` Suporte técnico, se `-support` estiver definido como `enable`
Diariamente (por padrão, enviado entre 12:00 e 1:00 como uma mensagem de desempenho), se o `-perf` parâmetro estiver definido como `true`	Endereços especificados no endereço -parceiro» Suporte técnico, se `-support` estiver definido como `enable`
Semanal (por padrão, enviado domingo entre as 12:00h e as 1:00h)	Endereços especificados em `-partner-address` Suporte técnico, se `-support` estiver definido como `enable`

Mensagens acionadas manualmente

Você pode iniciar ou reenviar manualmente uma mensagem do AutoSupport.

Quando a mensagem é enviada	Onde a mensagem é enviada
Você inicia manualmente uma mensagem usando o `system node autosupport invoke` comando	Se um URI for especificado usando o `-uri` parâmetro no `system node autosupport invoke` comando, a mensagem será enviada para esse URI. Se `-uri` for omitido, a mensagem é enviada para os endereços especificados em `-to` e `-partner -address`. A mensagem também é enviada para o suporte técnico se `-support` estiver definido como `enable`.

Quando a mensagem é enviada	Onde a mensagem é enviada
Você inicia manualmente uma mensagem usando o `system node autosupport invoke-core-upload` comando	Se um URI é especificado usando o `-uri` parâmetro no `system node autosupport invoke-core-upload` comando, a mensagem é enviada para esse URI, e o arquivo de despejo do núcleo é carregado para o URI. Se `-uri` for omitido `system node autosupport invoke-core-upload` no comando, a mensagem é enviada para o suporte técnico e o arquivo de despejo do núcleo é enviado para o site de suporte técnico. Ambos os cenários requerem que `-support` esteja definido como `enable` e `-transport` definido como `https` ou `http`. Devido ao grande tamanho dos arquivos de despejo de núcleo, a mensagem não é enviada para os endereços especificados nos `-to` parâmetros e. `-partner-addresses`
Você inicia manualmente uma mensagem usando o `system node autosupport invoke-performance-archive` comando	Se um URI for especificado usando o `-uri` parâmetro no `system node autosupport invoke-performance-archive` comando, a mensagem será enviada para esse URI e o arquivo de arquivo de desempenho será carregado para o URI. Se `-uri` for omitido `system node autosupport invoke-performance-archive` no , a mensagem será enviada para o suporte técnico e o arquivo de arquivo de desempenho será carregado no site de suporte técnico. Ambos os cenários requerem que `-support` esteja definido como `enable` e `-transport` definido como `https` ou `http`. Devido ao grande tamanho dos arquivos de arquivamento de desempenho, a mensagem não é enviada para os endereços especificados nos `-to` parâmetros e. `-partner-addresses`
Você reenvia manualmente uma mensagem passada usando o `system node autosupport history retransmit` comando	Apenas para o URI que você especificar no `-uri` parâmetro do `system node autosupport history retransmit` comando

Mensagens acionadas pelo suporte técnico

O suporte técnico pode solicitar mensagens do AutoSupport usando o recurso AutoSupport OnDemand.

Quando a mensagem é enviada	Onde a mensagem é enviada
Quando o AutoSupport obtém instruções de entrega para gerar novas mensagens AutoSupport	Endereços especificados em `-partner-address` Suporte técnico, se `-support` estiver definido como `enable` e `-transport` estiver definido como `https`
Quando o AutoSupport obtém instruções de entrega para reenviar mensagens passadas do AutoSupport	Suporte técnico, se `-support` estiver definido como `enable` e `-transport` estiver definido como `https`
Quando o AutoSupport obtém instruções de entrega para gerar novas mensagens AutoSupport que carregam arquivos de despejo de memória ou arquivo de desempenho	Suporte técnico, se `-support` estiver definido como `enable` e `-transport` estiver definido como `https`. O despejo de memória ou arquivo de desempenho é carregado para o site de suporte técnico.

Como o AutoSupport cria e envia mensagens acionadas por eventos

O AutoSupport cria mensagens AutoSupport acionadas por eventos quando o EMS processa um evento de acionamento. Uma mensagem do AutoSupport acionada por evento alerta os destinatários para problemas que exigem ação corretiva e contém apenas informações relevantes para o problema. Você pode personalizar o conteúdo a incluir e quem recebe as mensagens.

O AutoSupport usa o seguinte processo para criar e enviar mensagens AutoSupport acionadas por eventos:

1. Quando o EMS processa um evento de ativação, o EMS envia um pedido ao AutoSupport.

   Um evento de gatilho é um evento EMS com um destino AutoSupport e um nome que começa com um `callhome.` prefixo.

2. O AutoSupport cria uma mensagem AutoSupport acionada por evento.

   O AutoSupport coleta informações básicas e de solução de problemas de subsistemas associados ao gatilho para criar uma mensagem que inclua apenas informações relevantes para o evento de acionamento.

   Um conjunto padrão de subsistemas é associado a cada gatilho. No entanto, você pode optar por associar subsistemas adicionais a um gatilho usando o `system node autosupport trigger modify` comando.

3. O AutoSupport envia a mensagem AutoSupport acionada por evento aos destinatários definidos pelo `system node autosupport modify` comando com os `-to` parâmetros , `-noteto`, `-partner -address` e . `-support`

   Você pode ativar e desativar a entrega de mensagens do AutoSupport para gatilhos específicos usando o `system node autosupport trigger modify` comando com os `-to` parâmetros e. `-noteto`

Exemplo de dados enviados para um evento específico

O `storage shelf PSU failed` evento EMS aciona uma mensagem que contém dados básicos dos subsistemas obrigatório, arquivos de log, armazenamento, RAID, HA, Plataforma e rede e dados de solução de problemas dos subsistemas obrigatório, arquivos de log e armazenamento.

Você decide que deseja incluir dados sobre NFS em qualquer mensagem do AutoSupport enviada em resposta a um evento futuro `storage shelf PSU failed`. Digite o seguinte comando para habilitar dados em nível de solução de problemas para NFS para `callhome.shlf.ps.fault` o evento:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Observe que o `callhome.` prefixo é descartado do `callhome.shlf.ps.fault` evento quando você usa os `system node autosupport trigger` comandos, ou quando referenciado por eventos AutoSupport e EMS na CLI.

Tipos de mensagens AutoSupport e seu conteúdo

As mensagens AutoSupport contêm informações de status sobre subsistemas suportados. Aprender o que as mensagens do AutoSupport contêm pode ajudá-lo a interpretar ou responder às mensagens que você recebe em e-mail ou exibição no site do consultor digital.

Tipo de mensagem	Tipo de dados que a mensagem contém
Acionado por evento	Arquivos contendo dados sensíveis ao contexto sobre o subsistema específico em que o evento ocorreu
Diariamente	Ficheiros de registo
Desempenho	Dados de desempenho amostrados durante as 24 horas anteriores
Semanalmente	Dados de configuração e status

Tipo de mensagem	Tipo de dados que a mensagem contém
Acionado pelo `system node autosupport invoke` comando	Depende do valor especificado no `-type` parâmetro: • `test` envia uma mensagem acionada pelo usuário com alguns dados básicos. Essa mensagem também aciona uma resposta automática de e-mail do suporte técnico para qualquer endereço de e-mail especificado, usando a `-to` opção, para que você possa confirmar que as mensagens do AutoSupport estão sendo recebidas. • `performance` envia dados de desempenho. • `all` envia uma mensagem acionada pelo usuário com um conjunto completo de dados semelhante à mensagem semanal, incluindo dados de solução de problemas de cada subsistema. O suporte técnico normalmente solicita essa mensagem.
Acionado pelo `system node autosupport invoke-core-upload` comando	Arquivos de despejo de núcleo para um nó
Acionado pelo `system node autosupport invoke-performance-archive` comando	Arquivos de arquivamento de desempenho por um período de tempo especificado
Acionado por AutoSupport OnDemand	O AutoSupport OnDemand pode solicitar novas mensagens ou mensagens anteriores: • As novas mensagens, dependendo do tipo de coleção AutoSupport, podem ser `test`, `all` ou `performance`. • As mensagens anteriores dependem do tipo de mensagem que é reenviada. O AutoSupport OnDemand pode solicitar novas mensagens que carreguem os seguintes arquivos para o site de suporte da NetApp em "mysupport.NetApp.com": • Despejo de memória • Arquivamento de performance

Ver subsistemas AutoSupport

Cada subsistema fornece informações básicas e de solução de problemas que o

AutoSupport usa para suas mensagens. Cada subsistema também está associado a eventos de gatilho que permitem que o AutoSupport colete apenas informações relevantes para o evento de acionamento.

O AutoSupport coleta conteúdo sensível ao contexto.

Passos

1. Exibir informações sobre subsistemas e eventos de acionamento:

```
system node autosupport trigger show
```

Orçamentos de tamanho e tempo da AutoSupport

O AutoSupport coleta informações, organizadas por subsistema, e impõe um orçamento de tamanho e tempo para o conteúdo de cada subsistema. À medida que os sistemas de storage crescem, os orçamentos da AutoSupport fornecem controle sobre a carga útil da AutoSupport, que por sua vez fornece entrega dimensionável de dados da AutoSupport.

O AutoSupport pára de coletar informações e trunca o conteúdo do AutoSupport se o conteúdo do subsistema exceder seu tamanho ou orçamento de tempo. Se o conteúdo não puder ser truncado facilmente (por exemplo, arquivos binários), o AutoSupport omite o conteúdo.

Você deve modificar o tamanho padrão e os orçamentos de tempo somente se solicitado pelo suporte da NetApp. Você também pode revisar o tamanho padrão e os orçamentos de tempo dos subsistemas usando o `autosupport manifest show` comando.

Arquivos enviados em mensagens AutoSupport acionadas por evento

As mensagens AutoSupport acionadas por evento contêm apenas informações básicas e de solução de problemas de subsistemas associados ao evento que fez com que o AutoSupport gerasse a mensagem. Os dados específicos ajudam os parceiros de suporte e suporte da NetApp a solucionar o problema.

O AutoSupport usa os seguintes critérios para controlar o conteúdo em mensagens AutoSupport acionadas por evento:

- Quais subsistemas estão incluídos

  Os dados são agrupados em subsistemas, incluindo subsistemas comuns, como arquivos de log e subsistemas específicos, como RAID. Cada evento aciona uma mensagem que contém apenas os dados de subsistemas específicos.

- O nível de detalhe de cada subsistema incluído

  Os dados para cada subsistema incluído são fornecidos em um nível básico ou de solução de problemas.

Você pode visualizar todos os eventos possíveis e determinar quais subsistemas estão incluídos nas mensagens sobre cada evento usando o `system node autosupport trigger show` comando com o `-instance` parâmetro.

Além dos subsistemas que são incluídos por padrão para cada evento, você pode adicionar subsistemas adicionais em um nível básico ou de solução de problemas usando o `system node autosupport trigger modify` comando.

Arquivos de log enviados em mensagens do AutoSupport

As mensagens do AutoSupport podem conter vários arquivos de log-chave que permitem que a equipe de suporte técnico analise a atividade recente do sistema.

Todos os tipos de mensagens do AutoSupport podem incluir os seguintes arquivos de log quando o subsistema arquivos de log está habilitado:

Ficheiro de registo	Quantidade de dados incluídos no arquivo
• Arquivos de log do `/mroot/etc/log/mlog/` diretório • O ficheiro de registo DE MENSAGENS	Somente novas linhas adicionadas aos logs desde a última mensagem AutoSupport até um máximo especificado. Isso garante que as mensagens do AutoSupport tenham dados exclusivos e relevantes, não sobrepostos. (Os arquivos de log de parceiros são a exceção; para parceiros, os dados máximos permitidos são incluídos.)
• Arquivos de log do `/mroot/etc/log/shelflog/` diretório • Arquivos de log do `/mroot/etc/log/acp/` diretório • Dados de registo do sistema de gestão de eventos (EMS)	As linhas de dados mais recentes até um máximo especificado.

O conteúdo das mensagens do AutoSupport pode mudar entre as versões do ONTAP.

Arquivos enviados em mensagens AutoSupport semanais

As mensagens AutoSupport semanais contêm dados adicionais de configuração e status que são úteis para rastrear alterações no seu sistema ao longo do tempo.

As seguintes informações são enviadas em mensagens AutoSupport semanais:

- Informações básicas sobre cada subsistema
- Conteúdo de arquivos de diretório selecionados `/mroot/etc`
- Ficheiros de registo
- Saída de comandos que fornecem informações do sistema
- Informações adicionais, incluindo informações de banco de dados replicado (RDB), estatísticas de serviço e muito mais

Como o AutoSupport OnDemand obtém instruções de entrega do suporte técnico

O AutoSupport OnDemand se comunica periodicamente com o suporte técnico para obter instruções de entrega para enviar, reenviar e recusar mensagens AutoSupport, bem como carregar arquivos grandes para o site de suporte da NetApp. O AutoSupport OnDemand permite que as mensagens do AutoSupport sejam enviadas sob demanda em vez de esperar que a tarefa AutoSupport semanal seja executada.

O AutoSupport OnDemand consiste nos seguintes componentes:

- Cliente AutoSupport OnDemand que é executado em cada nó
- Serviço do AutoSupport OnDemand que reside no suporte técnico

O cliente do AutoSupport OnDemand faz periodicamente pesquisas no serviço do AutoSupport OnDemand para obter instruções de entrega do suporte técnico. Por exemplo, o suporte técnico pode usar o serviço OnDemand do AutoSupport para solicitar que uma nova mensagem do AutoSupport seja gerada. Quando o cliente AutoSupport OnDemand executa o serviço AutoSupport OnDemand, o cliente obtém as instruções de entrega e envia a nova mensagem AutoSupport sob demanda conforme solicitado.

O AutoSupport OnDemand está ativado por padrão. No entanto, o AutoSupport OnDemand depende de algumas configurações do AutoSupport para continuar se comunicando com o suporte técnico. O AutoSupport OnDemand se comunica automaticamente com o suporte técnico quando os seguintes requisitos são atendidos:

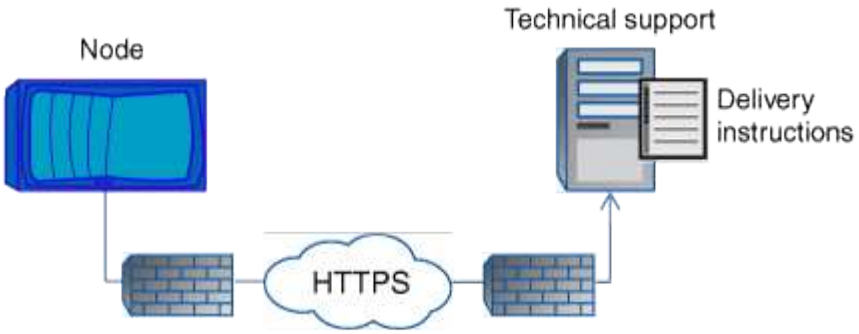
- O AutoSupport está ativado.
- O AutoSupport está configurado para enviar mensagens ao suporte técnico.
- O AutoSupport está configurado para utilizar o protocolo de transporte HTTPS.

O cliente AutoSupport OnDemand envia solicitações HTTPS para o mesmo local de suporte técnico para o qual as mensagens AutoSupport são enviadas. O cliente AutoSupport OnDemand não aceita conexões de entrada.

O AutoSupport OnDemand usa a conta de usuário "'AutoSupport'" para se comunicar com o suporte técnico. O ONTAP impede que você exclua essa conta.

Se você quiser desativar o AutoSupport OnDemand, mas manter o AutoSupport habilitado, use o comando: Link:https://docs.NetApp.com/US-en/ONTAP-cli/system-node-AutoSupport-moderd.html[`system node autosupport modify -ondemand-state disable`.

A ilustração a seguir mostra como o AutoSupport OnDemand envia solicitações HTTPS para o suporte técnico para obter instruções de entrega.



As instruções de entrega podem incluir pedidos para que a AutoSupport faça o seguinte:

- Gerar novas mensagens AutoSupport.

  O suporte técnico pode solicitar novas mensagens do AutoSupport para ajudar a triagem de problemas.

- Gere novas mensagens do AutoSupport que carregam arquivos de despejo de memória ou arquivos de arquivo de desempenho para o site de suporte do NetApp.

  O suporte técnico pode solicitar arquivos de despejo de núcleo ou arquivamento de desempenho para ajudar a triagem de problemas.

- Retransmita mensagens AutoSupport geradas anteriormente.

  Esta solicitação acontece automaticamente se uma mensagem não for recebida devido a uma falha de entrega.

- Desative a entrega de mensagens AutoSupport para eventos de gatilho específicos.

  O suporte técnico pode desativar a entrega de dados que não são usados.

Estrutura das mensagens AutoSupport enviadas por e-mail

Quando uma mensagem AutoSupport é enviada por e-mail, a mensagem tem um assunto padrão, um corpo breve e um anexo grande em formato de arquivo 7z que contém os dados.

Se o AutoSupport estiver configurado para ocultar dados privados, certas informações, como o nome do host, serão omitidas ou mascaradas no cabeçalho, assunto, corpo e anexos.

Assunto

A linha de assunto das mensagens enviadas pelo mecanismo AutoSupport contém uma cadeia de texto que identifica o motivo da notificação. O formato da linha de assunto é o seguinte:

Notificação de Grupo HA de *Nome_do_sistema* (*mensagem*) *gravidade*

- *Nome_do_sistema* é o nome do host ou o ID do sistema, dependendo da configuração do AutoSupport

Corpo

O corpo da mensagem AutoSupport contém as seguintes informações:

- Data e carimbo de data/hora da mensagem
- Versão do ONTAP no nó que gerou a mensagem
- ID do sistema, número de série e nome do host do nó que gerou a mensagem
- Número de sequência AutoSupport
- Nome e localização do contacto SNMP, se especificado
- ID do sistema e nome do host do partnernode HA

Ficheiros anexados

As informações-chave de uma mensagem AutoSupport estão contidas em arquivos compatados em um arquivo 7z chamado `body.7z` e anexado à mensagem.

Os arquivos contidos no anexo são específicos para o tipo de mensagem AutoSupport.

Tipos de gravidade do AutoSupport

As mensagens do AutoSupport têm tipos de gravidade que ajudam a entender o propósito de cada mensagem - por exemplo, chamar a atenção imediata para um problema de emergência ou apenas para fornecer informações.

As mensagens têm uma das seguintes gravidades:

- **Alerta**: As mensagens de alerta indicam que um evento de nível superior próximo pode ocorrer se você não tomar alguma ação.

  Você deve tomar uma ação contra mensagens de alerta dentro de 24 horas.

- **Emergência**: As mensagens de emergência são exibidas quando ocorre uma interrupção.

  Você deve tomar uma ação contra mensagens de emergência imediatamente.

- **Erro**: As condições de erro indicam o que pode acontecer se você ignorar.
- **Aviso**: Condição normal, mas significativa.
- **Info**: A mensagem informativa fornece detalhes sobre o problema, que você pode ignorar.
- **Debug**: Mensagens no nível de depuração fornecem instruções que você deve executar.

Se a organização de suporte interno receber mensagens do AutoSupport por e-mail, a gravidade será exibida na linha de assunto da mensagem de e-mail.

Obter descrições de mensagens do AutoSupport

As descrições das mensagens do AutoSupport que você recebe estão disponíveis através do Tradutor Syslog do ONTAP.

Passos

1. Vá para "Syslog Translator".
2. No campo **Liberação**, insira a versão do ONTAP que você está usando. No campo **Search String**, digite "callhome". Selecione **Traduzir**.
3. O Syslog Translator listará alfabeticamente todos os eventos que correspondem à cadeia de carateres da mensagem que você inseriu.

Comandos para gerenciar o AutoSupport

Você usa os `system node autosupport` comandos para alterar ou exibir a configuração do AutoSupport, exibir informações sobre mensagens AutoSupport anteriores e enviar, reenviar ou cancelar uma mensagem do AutoSupport.

Configurar o AutoSupport

Se você quiser…	Use este comando…
Controle se quaisquer mensagens AutoSupport são enviadas	`system node autosupport modify` com o `-state` parâmetro
Controlar se as mensagens AutoSupport são enviadas para o suporte técnico	`system node autosupport modify` com o `-support` parâmetro
Configure o AutoSupport ou modifique a configuração do AutoSupport	`system node autosupport modify`
Ative e desative as mensagens do AutoSupport para sua organização de suporte interno para eventos de acionamento individuais e especifique relatórios de subsistema adicionais a serem incluídos nas mensagens enviadas em resposta a eventos de acionamento individuais	`system node autosupport trigger modify`

Exibir informações sobre a configuração do AutoSupport

Se você quiser…	Use este comando…
Apresentar a configuração do AutoSupport	`system node autosupport show` com o `-node` parâmetro
Veja um resumo de todos os endereços e URLs que recebem mensagens do AutoSupport	`system node autosupport destinations show`
Exiba quais mensagens do AutoSupport são enviadas para sua organização interna de suporte para eventos de acionamento individuais	`system node autosupport trigger show`
Apresentar o estado da configuração do AutoSupport, bem como a entrega para vários destinos	`system node autosupport check show`
Apresentar o estado detalhado da configuração do AutoSupport, bem como a entrega para vários destinos	`system node autosupport check show-details`

Exibir informações sobre mensagens anteriores do AutoSupport

Se você quiser…	Use este comando…
Exiba informações sobre uma ou mais das 50 mensagens AutoSupport mais recentes	`system node autosupport history show`

Se você quiser…	Use este comando…
Exiba informações sobre mensagens recentes do AutoSupport geradas para carregar arquivos de despejo de memória ou arquivamento de desempenho para o site de suporte técnico ou um URI especificado	`system node autosupport history show-upload-details`
Visualize as informações nas mensagens do AutoSupport, incluindo o nome e o tamanho de cada arquivo coletado para a mensagem, juntamente com quaisquer erros	`system node autosupport manifest show`

Enviar, reenviar ou cancelar mensagens AutoSupport

Se você quiser…	Use este comando…
Retransmita uma mensagem AutoSupport armazenada localmente, identificada pelo seu número de sequência AutoSupport Se você retransmitir uma mensagem do AutoSupport e se o suporte já recebeu essa mensagem, o sistema de suporte não criará um caso duplicado. Se, por outro lado, o suporte não recebeu essa mensagem, o sistema AutoSupport analisará a mensagem e criará um caso, se necessário.	`system node autosupport history retransmit`
Gerar e enviar uma mensagem AutoSupport - por exemplo, para fins de teste	`system node autosupport invoke` Use o `-force` parâmetro para enviar uma mensagem mesmo que o AutoSupport esteja desativado. Use o `-uri` parâmetro para enviar a mensagem para o destino especificado em vez do destino configurado.
Cancelar uma mensagem AutoSupport	`system node autosupport history cancel`

Informações relacionadas

"Referência do comando ONTAP"

Informações incluídas no manifesto AutoSupport

O manifesto do AutoSupport fornece uma visualização detalhada dos arquivos coletados para cada mensagem do AutoSupport. O manifesto AutoSupport também inclui informações sobre erros de coleta quando o AutoSupport não consegue coletar os

arquivos de que ele precisa.

O manifesto AutoSupport inclui as seguintes informações:

- Número de sequência da mensagem AutoSupport
- Quais arquivos AutoSupport incluídos na mensagem AutoSupport
- Tamanho de cada arquivo, em bytes
- Status da coleção de manifesto do AutoSupport
- Descrição do erro, se o AutoSupport não conseguir recolher um ou mais ficheiros

Você pode exibir o manifesto do AutoSupport usando o `system node autosupport manifest show` comando.

O manifesto do AutoSupport é incluído com todas as mensagens do AutoSupport e apresentado em formato XML, o que significa que você pode usar um visualizador XML genérico para lê-lo ou visualizá-lo usando o portal do Consultor Digital.

Plano

Prepare-se para usar o AutoSupport

Você pode configurar um cluster do ONTAP para entregar mensagens do AutoSupport ao NetApp. Como parte disso, você também pode enviar uma cópia das mensagens para endereços de e-mail locais, normalmente dentro da sua organização. Você deve se preparar para configurar o AutoSupport revisando as opções disponíveis.

Entregar mensagens AutoSupport ao NetApp

As mensagens AutoSupport podem ser entregues ao NetApp usando protocolos HTTPS ou SMTP. Começando com ONTAP 9.15,1, você também pode usar TLS com SMTP.

Use HTTPS sempre que possível para comunicação com o AutoSupport OnDemand e upload de arquivos grandes.

Observe também o seguinte:

- Apenas um canal de entrega ao NetApp pode ser configurado para as mensagens AutoSupport. Não é possível usar dois protocolos para entregar mensagens AutoSupport ao NetApp.
- O AutoSupport limita o tamanho máximo do arquivo para cada protocolo. Se o tamanho de uma mensagem AutoSupport exceder o limite configurado, o AutoSupport entrega o máximo possível da mensagem, mas ocorrerá truncamento.
- Você pode alterar o tamanho máximo do arquivo, se necessário. Saiba mais sobre o[`system node autosupport modify` comando ONTAP na referência de comando.
- Ambos os protocolos podem ser transportados em IPv4 ou IPv6 com base na família de endereços para a qual o nome resolve.
- A conexão TCP estabelecida pelo ONTAP para enviar mensagens AutoSupport é temporária e de curta duração.

HTTPS

Isso fornece os recursos mais robustos. Observe o seguinte:

- O AutoSupport OnDemand e a transferência de arquivos grandes são suportados.
- Uma solicitação HTTPS PUT é tentada primeiro. Se a solicitação falhar durante a transmissão, a solicitação será reiniciada onde ela parou.
- Se o servidor não suportar PUT, o método HTTPS POST é usado.
- O limite padrão para transferências HTTPS é de 50 MB.
- O protocolo HTTPS utiliza a porta 443.

SMTP

Como regra geral, você deve usar SMTP somente se HTTPS não for permitido ou não for suportado. Observe o seguinte:

- O AutoSupport OnDemand e as transferências de arquivos grandes não são suportadas.
- Se as credenciais de login SMTP estiverem configuradas, elas serão enviadas sem criptografia e na opção Limpar.
- O limite padrão para transferências é de 5 MB.
- O protocolo SMTP não protegido usa a porta 25.

Melhore a segurança SMTP com TLS

Ao usar SMTP, todo o tráfego é descriptografado e pode ser facilmente intercetado e lido. Começando com ONTAP 9.15,1 você também pode usar TLS com SMTP (SMTPS). Neste caso, *explícito TLS* é usado que ativa o canal seguro após a conexão TCP ser estabelecida.

A seguinte porta é normalmente utilizada para SMTPS: Porta 587

Considerações de configuração adicionais

Há algumas considerações adicionais ao configurar o AutoSupport.

Para obter mais informações sobre os comandos relevantes para estas considerações, "Configure o AutoSupport"consulte .

Envie uma cópia local usando e-mail

Independentemente do protocolo usado para entregar mensagens AutoSupport ao NetApp, você também pode enviar uma cópia de cada mensagem para um ou mais endereços de e-mail locais. Por exemplo, você pode enviar mensagens para sua organização interna de suporte ou uma organização parceira.

> Se você entregar mensagens para o NetApp usando SMTP (ou SMTPS) e enviar cópias de e-mail locais dessas mensagens, a mesma configuração do servidor de e-mail será usada.

Proxy HTTP

Dependendo da configuração da rede, o protocolo HTTPS pode exigir configuração adicional de um URL de proxy. Se o HTTPS for usado para enviar mensagens do AutoSupport para o suporte técnico e você tiver um proxy, você deverá identificar o URL do proxy. Se o proxy usar uma porta diferente da padrão (porta 3128), você poderá especificar a porta para esse proxy. Você também pode especificar opcionalmente um nome de

usuário e senha para autenticação de proxy.

Instale o certificado do servidor

Com TLS (HTTPS ou SMTPS), o certificado baixado do servidor é validado pelo ONTAP com base no certificado CA raiz. Antes de usar HTTPS ou SMTPS, você precisa garantir que o certificado raiz esteja instalado no ONTAP e que o ONTAP possa validar o certificado do servidor. Essa validação é realizada com base na CA que assinou o certificado do servidor.

O ONTAP inclui um grande número de certificados de CA raiz pré-instalados. Em muitos casos, o certificado para o seu servidor será imediatamente reconhecido pelo ONTAP sem configuração adicional. Dependendo de como o certificado do servidor foi assinado, talvez seja necessário instalar um certificado de CA raiz e quaisquer certificados intermediários.

Use o procedimento a seguir para instalar o certificado, se necessário. Você deve instalar todos os certificados necessários no nível do cluster.

Exemplo 35. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Selecione → ao lado de **certificados**.
4. Na guia **autoridades de certificação confiáveis**, clique em **Adicionar**.
5. Clique em **Importar** e selecione o arquivo de certificado.
6. Complete os parâmetros de configuração para o seu ambiente.
7. Clique em **Add**.

CLI

1. Inicie a instalação:

```
security certificate install -type server-ca
```

2. Procure a seguinte mensagem do console:

```
Please enter Certificate: Press <Enter> when done
```

3. Abra o arquivo de certificado com um editor de texto.
4. Copie o certificado inteiro, incluindo as seguintes linhas:

```
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
```

5. Cole o certificado no terminal após o prompt de comando.
6. Pressione **Enter** para concluir a instalação.
7. Confirme se o certificado está instalado executando um dos seguintes comandos:

```
security certificate show-user-installed
```

```
security certificate show
```

Informações relacionadas

- "Configure o AutoSupport"

Configure o AutoSupport

Você pode configurar um cluster do ONTAP para entregar mensagens do AutoSupport ao suporte técnico da NetApp e enviar cópias de e-mail para sua organização de suporte interno. Como parte disso, você também pode testar a configuração antes de usá-la em um ambiente de produção.

Sobre esta tarefa

A partir do ONTAP 9.5, você ativa e configura o AutoSupport para todos os nós de um cluster simultaneamente. Quando um novo nó entra no cluster, o nó herda automaticamente a mesma configuração do AutoSupport. Para dar suporte a isso, o escopo do comando CLI `system node autosupport modify` é no nível do cluster. A `-node` opção de comando é mantida para compatibilidade com versões anteriores, mas é ignorada.

> No ONTAP 9.4 e versões anteriores, o comando `system node autosupport modify` é específico para cada nó. Se o cluster estiver executando o ONTAP 9.4 ou anterior, será necessário habilitar e configurar o AutoSupport em cada nó do cluster.

Antes de começar

A configuração de transporte recomendada para entregar mensagens AutoSupport para o NetApp é HTTPS (HTTP com TLS). Esta opção fornece os recursos mais robustos e a melhor segurança.

Consulte "Prepare-se para usar o AutoSupport" para obter mais informações antes de configurar o cluster do ONTAP.

Passos

1. Certifique-se de que o AutoSupport está ativado:

   ```
   system node autosupport modify -state enable
   ```

2. Se você quiser que o suporte técnico da NetApp receba mensagens do AutoSupport, use o seguinte comando:

   ```
   system node autosupport modify -support enable
   ```

   Você deve habilitar essa opção se quiser habilitar o AutoSupport para trabalhar com o AutoSupport OnDemand ou se quiser fazer upload de arquivos grandes, como arquivos de despejo de núcleo e arquivamento de desempenho, para suporte técnico ou um URL especificado.

   > O AutoSupport OnDemand é ativado por padrão e funcional quando configurado para enviar mensagens para suporte técnico usando o protocolo de transporte HTTPS.

3. Se você tiver habilitado o suporte técnico do NetApp para receber mensagens do AutoSupport, especifique qual protocolo de transporte usar para essas mensagens.

   Você pode escolher entre as seguintes opções:

Se você quiser…	Em seguida, defina os seguintes parâmetros `system node autosupport modify` do comando…
Utilize o protocolo HTTPS predefinido	a. Defina `-transport` para `https`. b. Se você usar um proxy, defina `-proxy-url` o URL do seu proxy. Esta configuração suporta a comunicação com o AutoSupport OnDemand e carregamentos de ficheiros grandes.
Utilize SMTP	Defina `-transport` para `smtp`. Esta configuração não suporta o AutoSupport OnDemand ou carregamentos de ficheiros grandes.

4. Se você quiser que sua organização de suporte interna ou um parceiro de suporte recebam mensagens do AutoSupport, execute as seguintes ações:
   a. Identifique os destinatários em sua organização definindo os seguintes parâmetros `system node autosupport modify` do comando:

Definir este parâmetro…	Para isso…
`-to`	Até cinco endereços de e-mail individuais separados por vírgulas ou listas de distribuição em sua organização de suporte interno que receberão as principais mensagens do AutoSupport
`-noteto`	Até cinco endereços de e-mail individuais separados por vírgulas ou listas de distribuição em sua organização de suporte interno que receberão uma versão abreviada das principais mensagens AutoSupport projetadas para telefones celulares e outros dispositivos móveis
`-partner-address`	Até cinco endereços de e-mail individuais separados por vírgulas ou listas de distribuição na sua organização de parceiros de suporte que receberão todas as mensagens do AutoSupport

   b. Verifique se os endereços estão corretamente configurados listando os destinos usando o `system node autosupport destinations show` comando.
5. Se você configurou os endereços de destinatário para sua organização de suporte interno na etapa anterior ou escolheu o transporte SMTP para mensagens para suporte técnico, configure o SMTP definindo os seguintes parâmetros `system node autosupport modify` do comando:
   - Defina `-mail-hosts` como um ou mais hosts de e-mail, separados por vírgulas.

     Você pode definir um máximo de cinco.

Você pode configurar um valor de porta para cada host de e-mail especificando dois pontos e um número de porta após o nome do host de e-mail: Por exemplo, `mymailhost.example.com:5678`, onde 5678 é a porta para o host de e-mail.

- Defina `-from` para o endereço de e-mail que envia a mensagem AutoSupport.

6. Configure o DNS.
7. Opcionalmente, adicione opções de comando se você quiser alterar configurações específicas:

Se você quiser fazer isso…	Em seguida, defina os seguintes parâmetros `system node autosupport modify` do comando…
Oculte dados privados removendo, mascarando ou codificando dados confidenciais nas mensagens	Defina `-remove-private-data` para `true`. Se você mudar de `false` para `true`, todo o histórico do AutoSupport e todos os arquivos associados serão excluídos.
Pare de enviar dados de desempenho em mensagens AutoSupport periódicas	Defina `-perf` para `false`.

8. Se você estiver usando SMTP para entregar mensagens do AutoSupport ao NetApp, você pode opcionalmente ativar o TLS para maior segurança.
   a. Apresentar os valores disponíveis para o novo parâmetro:

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

   b. Ativar TLS para envio de mensagens SMTP:

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

   c. Apresentar a configuração atual:

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. Verificar a configuração geral utilizando o `system node autosupport show` comando com o `-node` parâmetro.
10. Verifique a operação do AutoSupport usando o `system node autosupport check show` comando.

    Se algum problema for relatado, use o `system node autosupport check show-details` comando para exibir mais informações.

11. Teste se as mensagens AutoSupport estão sendo enviadas e recebidas:
    a. Utilize o `system node autosupport invoke` comando com o `-type` parâmetro definido para `test`:

```
cluster1::> system node autosupport invoke -type test -node node1
```

b. Confirme se o NetApp está recebendo suas mensagens do AutoSupport:

```
system node autosupport history show -node local
```

O estado da mensagem AutoSupport de saída mais recente deverá eventualmente mudar para para para `sent-successful` todos os destinos de protocolo apropriados.

c. Opcionalmente, confirme se as mensagens do AutoSupport estão sendo enviadas para sua organização de suporte interna ou para seu parceiro de suporte verificando o e-mail de qualquer endereço configurado para os `-to` parâmetros , `-noteto` ou `-partner-address` do `system node autosupport modify` comando.

Informações relacionadas

- "Prepare-se para usar o AutoSupport"

Configurar

Gerir as definições do AutoSupport

Pode utilizar o Gestor do sistema para gerir as definições da sua conta AutoSupport.

Para obter mais informações sobre as opções de configuração do AutoSupport, incluindo as configurações que não estão disponíveis no Gerenciador do sistema, consulte `system-node-autosupport-modify` no "Referência do comando ONTAP".

Ver definições do AutoSupport

Você pode usar o Gerenciador do sistema para exibir as configurações da sua conta do AutoSupport.

Passos

1. No System Manager, clique em **Cluster > Settings**.

   Na seção **AutoSupport**, as seguintes informações são exibidas:

   - Estado
   - Protocolo de transporte
   - Servidor proxy
   - Do endereço de e-mail

2. Na seção **AutoSupport**, selecione e, em seguida, selecione **mais opções**.

   São apresentadas informações adicionais sobre a ligação à AutoSupport e as definições de correio eletrónico. Além disso, o histórico de transferência de mensagens é listado.

Gerar e enviar dados AutoSupport

No Gerenciador de sistema, você pode iniciar a geração de mensagens do AutoSupport e escolher de qual nó ou nós de cluster os dados são coletados.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **AutoSupport**, selecione e, em seguida, selecione **Generate and Send**.
3. Introduza um assunto.
4. Marque a caixa de seleção em **coletar dados de** para especificar os nós dos quais coletar os dados.

Teste a conexão com o AutoSupport

No Gerenciador de sistema, você pode enviar uma mensagem de teste para verificar a conexão com o AutoSupport.

Passos

1. No System Manager, clique em **Cluster > Settings**.
2. Na seção **AutoSupport**, selecione e, em seguida, **testar conetividade**.
3. Introduza um assunto para a mensagem.

Ative ou desative o AutoSupport

O AutoSupport oferece benefícios de negócios comprovados para clientes da NetApp, incluindo identificação proativa de possíveis problemas de configuração e resolução acelerada de casos de suporte. O AutoSupport é ativado por padrão em novos sistemas. Se necessário, você pode usar o Gerenciador do sistema para desativar a capacidade do AutoSupport de monitorar a integridade do sistema de storage e enviar mensagens de notificação. Você pode ativar o AutoSupport novamente depois que ele tiver sido desativado.

Sobre esta tarefa

Antes de desativar o AutoSupport, você deve estar ciente de que você está desligando o sistema call-home do NetApp e você perderá os seguintes benefícios:

- **Monitoramento de integridade**: O AutoSupport monitora a integridade do seu sistema de storage e envia notificações ao suporte técnico e à sua organização de suporte interno.
- **Automação**: O AutoSupport automatiza a geração de relatórios de casos de suporte. A maioria dos casos de suporte são abertos automaticamente antes que os clientes percebam que há um problema.
- * Resolução mais rápida*: Os sistemas que enviam dados AutoSupport têm seus casos de suporte resolvidos pela metade do tempo em comparação aos casos para sistemas que não enviam dados AutoSupport.
- **Atualizações mais rápidas**: O AutoSupport capacita fluxos de trabalho de autoatendimento do cliente, como atualizações de versão, complementos, renovações e automação de atualizações de firmware no System Manager.
- **Mais funções**: Certas funções em outras ferramentas funcionam somente quando o AutoSupport está habilitado, por exemplo, alguns fluxos de trabalho no BlueXP .

Passos

1. Selecione **Cluster > Settings**.
2. Na secção **AutoSupport**, selecione e, em seguida, selecione **Desativar**.

3. Se quiser ativar o AutoSupport novamente, na seção **AutoSupport**, selecione e, em seguida, selecione **Enable**.

Suprimir a geração de casos de suporte

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para enviar uma solicitação ao AutoSupport para suprimir a geração de casos de suporte.

Sobre esta tarefa

Para suprimir a geração de casos de suporte, especifique os nós e o número de horas para os quais deseja que a supressão ocorra.

Suprimir casos de suporte pode ser especialmente útil se você não quiser que o AutoSupport crie casos automatizados enquanto estiver realizando manutenção em seus sistemas.

Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**, selecione e, em seguida, **suprimir geração de casos de suporte**.
3. Introduza o número de horas que pretende que a supressão ocorra.
4. Selecione os nós para os quais você deseja que a supressão ocorra.

Retomar a geração de casos de suporte

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para retomar a geração de casos de suporte do AutoSupport se ele tiver sido suprimido.

Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**, selecione e, em seguida, **Resume Support Case Generation**.
3. Selecione os nós para os quais deseja que a geração seja retomada.

Edite as definições do AutoSupport

Você pode usar o Gerenciador do sistema para modificar as configurações de conexão e e-mail da sua conta do AutoSupport.

Passos

1. Selecione **Cluster > Settings**.
2. Na seção **AutoSupport**, selecione e, em seguida, selecione **mais opções**.
3. Na seção **conexões** ou na seção **Email**, Edit selecione para modificar as configurações de qualquer seção.

Informações relacionadas

- "Prepare-se para usar o AutoSupport"
- "Configure o AutoSupport"

Suprimir a criação de casos AutoSupport durante as janelas de manutenção programada no ONTAP

A supressão de casos AutoSupport permite que você impeça que casos desnecessários sejam criados por mensagens AutoSupport que são acionadas durante janelas de

manutenção programada.

Passos

1. Invoque manualmente uma mensagem AutoSupport com a cadeia de texto `MAINT=xh` , onde `x` é a duração da janela de manutenção em horas. Substitua o <node> pelo nome do nó a partir do qual enviar a mensagem AutoSupport:

```
system node autosupport invoke -node <node> -message MAINT=xh
```

Informações relacionadas

- "Referência do comando ONTAP"
- "Como suprimir a criação automática de casos durante as janelas de manutenção programada"

Carregue ficheiros utilizando o AutoSupport

Carregue arquivos de despejo de memória

Quando um arquivo de despejo de memória é salvo, uma mensagem de evento é gerada. Se o serviço AutoSupport estiver ativado e configurado para enviar mensagens ao suporte do NetApp, uma mensagem AutoSupport será transmitida e uma confirmação automática por e-mail será enviada para você.

O que você vai precisar

- Você deve ter configurado o AutoSupport com as seguintes configurações:
  - O AutoSupport está ativado no nó.
  - O AutoSupport está configurado para enviar mensagens ao suporte técnico.
  - O AutoSupport está configurado para usar o protocolo de transporte HTTP ou HTTPS.

    O protocolo de transporte SMTP não é suportado ao enviar mensagens que incluam arquivos grandes, como arquivos de despejo de memória.

Sobre esta tarefa

Você também pode fazer o upload do arquivo de despejo do núcleo através do serviço AutoSupport em HTTPS usando o `system node autosupport invoke-core-upload` comando, se solicitado pelo suporte do NetApp.

"Como fazer upload de um arquivo para o NetApp"

Passos

1. Veja os arquivos de despejo de núcleo para um nó usando o `system node coredump show` comando.

   No exemplo a seguir, os arquivos de despejo do núcleo são exibidos para o nó local:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
--------- ------------------------------------------ -----
----------------
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Gere uma mensagem AutoSupport e carregue um arquivo de despejo de memória usando o `system node autosupport invoke-core-upload` comando.

   No exemplo a seguir, uma mensagem do AutoSupport é gerada e enviada para o local padrão, que é suporte técnico, e o arquivo de despejo de núcleo é carregado para o local padrão, que é o site de suporte do NetApp:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

   No exemplo a seguir, uma mensagem do AutoSupport é gerada e enviada para o local especificado no URI, e o arquivo de despejo do núcleo é carregado para o URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Carregue ficheiros de arquivo de desempenho

Você pode gerar e enviar uma mensagem do AutoSupport que contenha um arquivo de desempenho. Por padrão, o suporte técnico da NetApp recebe a mensagem AutoSupport e o arquivo de desempenho é carregado no site de suporte da NetApp. Você pode especificar um destino alternativo para a mensagem e upload.

O que você vai precisar

- Você deve ter configurado o AutoSupport com as seguintes configurações:
  - O AutoSupport está ativado no nó.
  - O AutoSupport está configurado para enviar mensagens ao suporte técnico.
  - O AutoSupport está configurado para usar o protocolo de transporte HTTP ou HTTPS.

    O protocolo de transporte SMTP não é suportado ao enviar mensagens que incluam arquivos grandes, como arquivos de arquivo de desempenho.

Sobre esta tarefa

Tem de especificar uma data de início para os dados de arquivo de desempenho que pretende carregar. A maioria dos sistemas de storage mantém arquivos de performance por duas semanas, permitindo que você especifique uma data de início há até duas semanas. Por exemplo, se hoje é 15 de janeiro, você pode

especificar uma data de início de 2 de janeiro.

Passo

1. Gere uma mensagem AutoSupport e carregue o arquivo de arquivo de desempenho usando o `system node autosupport invoke-performance-archive` comando.

   No exemplo a seguir, 4 horas de arquivos de arquivamento de desempenho de 12 de janeiro de 2015 são adicionados a uma mensagem do AutoSupport e carregados para o local padrão, que é o site de suporte do NetApp:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   No exemplo a seguir, 4 horas de arquivos de arquivo de desempenho a partir de 12 de janeiro de 2015 são adicionados a uma mensagem AutoSupport e carregados para o local especificado pelo URI:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

Solucionar problemas

Solucionar problemas do AutoSupport quando as mensagens não forem recebidas

Se o sistema não enviar a mensagem AutoSupport, você pode determinar se isso ocorre porque o AutoSupport não pode gerar a mensagem ou não pode entregar a mensagem.

Passos

1. Verifique o status de entrega das mensagens usando o `system node autosupport history show` comando.
2. Leia o estado.

Este estado	Meios
a inicializar	O processo de coleta está começando. Se este estado é temporário, tudo está bem. No entanto, se este estado persistir, há um problema.
falha na recolha	O AutoSupport não pode criar o conteúdo AutoSupport no diretório spool. Você pode ver o que o AutoSupport está tentando coletar digitando o `system node autosupport history show -detail` comando.
coleção em andamento	O AutoSupport está coletando conteúdo do AutoSupport. Você pode ver o que o AutoSupport está coletando digitando o `system node autosupport manifest show` comando.

Este estado	Meios
em fila de espera	As mensagens AutoSupport estão na fila para entrega, mas ainda não entregues.
transmissão	O AutoSupport está atualmente entregando mensagens.
enviado com sucesso	O AutoSupport entregou a mensagem com êxito. Você pode descobrir onde o AutoSupport entregou a mensagem digitando o `system node autosupport history show -delivery` comando.
ignorar	O AutoSupport não tem destinos para a mensagem. Você pode visualizar os detalhes da entrega inserindo o `system node autosupport history show -delivery` comando.
re-enfileirada	O AutoSupport tentou entregar mensagens, mas a tentativa falhou. Como resultado, o AutoSupport colocou as mensagens de volta na fila de entrega para outra tentativa. Você pode ver o erro digitando o `system node autosupport history show` comando.
falha na transmissão	O AutoSupport não conseguiu entregar a mensagem o número especificado de vezes e parou de tentar entregar a mensagem. Você pode ver o erro digitando o `system node autosupport history show` comando.
ondemand-ignore	A mensagem AutoSupport foi processada com sucesso, mas o serviço AutoSupport OnDemand optou por ignorá-la.

3. Execute uma das seguintes ações:

Para este estado	Faça isso
inicialização ou falha de coleta	Entre em Contato com o suporte da NetApp porque o AutoSupport não pode gerar a mensagem. Mencione o seguinte artigo da base de dados de Conhecimento: "O AutoSupport não consegue entregar: O estado está preso na inicialização"
ignorar, recolocar em fila ou falha na transmissão	Verifique se os destinos estão configurados corretamente para SMTP, HTTP ou HTTPS porque o AutoSupport não consegue entregar a mensagem.

Solucionar problemas de entrega de mensagens do AutoSupport através de HTTPS

Se o sistema não enviar a mensagem AutoSupport esperada e você estiver usando HTTPS ou o recurso Atualização automática não estiver funcionando, você poderá

verificar várias configurações para resolver o problema.

Antes de começar

Você deve ter confirmado a conetividade básica de rede e a pesquisa de DNS:

- Seu LIF de gerenciamento de nós precisa estar pronto para o status operacional e administrativo.
- Você deve ser capaz de fazer ping a um host em funcionamento na mesma sub-rede a partir do LIF de gerenciamento de cluster (não um LIF em nenhum dos nós).
- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster.
- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster usando o nome do host (não o endereço IP).

Sobre esta tarefa

Essas etapas são para casos em que você determinou que o AutoSupport pode gerar a mensagem, mas não pode entregar a mensagem por HTTPS.

Se você encontrar erros ou não conseguir concluir uma etapa neste procedimento, determine e solucione o problema antes de prosseguir para a próxima etapa.

Passos

1. Apresentar o estado detalhado do subsistema AutoSupport:

   `system node autosupport check show-details`

   Isso inclui verificar a conetividade com destinos do AutoSupport enviando mensagens de teste e fornecendo uma lista de possíveis erros nas configurações do AutoSupport.

2. Verifique o status do LIF de gerenciamento de nós:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   Os `status-oper` campos e `status-admin` devem retornar `up`.

3. Registre o nome da SVM, o nome LIF e o endereço IP LIF para uso posterior.
4. Certifique-se de que o DNS está ativado e configurado corretamente:

   ```
   vserver services name-service dns show
   ```

5. Solucione quaisquer erros retornados pela mensagem AutoSupport:

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   Para obter assistência para solucionar quaisquer erros retornados, consulte o "Guia de resolução ONTAP

AutoSupport (HTTPS de transporte e HTTP)".

6. Confirme se o cluster pode aceder aos servidores de que necessita e à Internet com sucesso:

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > O endereço `support.netapp.com` em si não responde ao ping/traceroute, mas as informações por salto são valiosas.

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   Se alguma dessas rotas não estiver funcionando, tente a mesma rota de um host em funcionamento na mesma sub-rede que o cluster, usando o `traceroute` utilitário ou `tracert` encontrado na maioria dos clientes de rede de terceiros. Em seguida, você pode determinar se o problema está na configuração da rede ou na configuração do cluster.

7. Se estiver a utilizar HTTPS para o protocolo de transporte AutoSupport, certifique-se de que o tráfego HTTPS pode sair da rede:

   a. Configure um cliente Web na mesma sub-rede que o LIF de gerenciamento de cluster.

      Certifique-se de que todos os parâmetros de configuração sejam os mesmos valores que para a configuração do AutoSupport, incluindo o uso do mesmo servidor proxy, nome de usuário, senha e porta.

   b. Acesso `https://support.netapp.com` com o cliente web.

      O acesso deve ser bem-sucedido. Caso contrário, verifique se todos os firewalls estão configurados corretamente para permitir tráfego HTTPS e DNS e se o servidor proxy está configurado corretamente. Para obter mais informações sobre como configurar a resolução de nomes estáticos para support.NetApp.com, consulte o artigo da base de dados de Conhecimento "Como uma ENTRADA DE HOST seria adicionada no ONTAP para support.NetApp.com?"

8. A partir do ONTAP 9.10.1 se você ativou o recurso Atualização automática, verifique se você tem conetividade HTTPS com os seguintes URLs adicionais:
   - https://support-sg-emea.NetApp.com
   - https://support-sg-naeast.NetApp.com
   - https://support-sg-nawest.NetApp.com

Solucionar problemas de entrega de mensagens do AutoSupport através de SMTP

Se o sistema não puder entregar mensagens AutoSupport por SMTP, você poderá verificar várias configurações para resolver o problema.

O que você vai precisar

Você deve ter confirmado a conetividade básica de rede e a pesquisa de DNS:

- Seu LIF de gerenciamento de nós precisa estar pronto para o status operacional e administrativo.
- Você deve ser capaz de fazer ping a um host em funcionamento na mesma sub-rede a partir do LIF de

gerenciamento de cluster (não um LIF em nenhum dos nós).

- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster.
- Você deve ser capaz de fazer ping a um host em funcionamento fora da sub-rede a partir do LIF de gerenciamento de cluster usando o nome do host (não o endereço IP).

Sobre esta tarefa

Essas etapas são para casos em que você determinou que o AutoSupport pode gerar a mensagem, mas não pode entregar a mensagem por SMTP.

Se você encontrar erros ou não conseguir concluir uma etapa neste procedimento, determine e solucione o problema antes de prosseguir para a próxima etapa.

Todos os comandos são inseridos na interface de linha de comando do ONTAP, a menos que especificado de outra forma.

Passos

1. Verifique o status do LIF de gerenciamento de nós:

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   Os `status-oper` campos e `status-admin` devem retornar `up`.

2. Registre o nome da SVM, o nome LIF e o endereço IP LIF para uso posterior.
3. Certifique-se de que o DNS está ativado e configurado corretamente:

   vserver services name-service dns show

4. Exibir todos os servidores configurados para serem usados pelo AutoSupport:

   system node autosupport show -fields mail-hosts

   Gravar todos os nomes de servidor exibidos.

5. Para cada servidor exibido pela etapa anterior, e `support.netapp.com`, certifique-se de que o servidor ou URL pode ser alcançado pelo nó:

   network traceroute -node local -destination *server_name*

   Se alguma dessas rotas não estiver funcionando, tente a mesma rota de um host em funcionamento na mesma sub-rede que o cluster, usando o utilitário "traceroute" ou "tracert" encontrado na maioria dos clientes de rede de terceiros. Isso ajuda você a determinar se o problema está na configuração da rede ou na configuração do cluster.

6. Faça login no host designado como host de e-mail e certifique-se de que ele possa atender solicitações SMTP:

   netstat -aAn|grep 25

   `25` É o número da porta SMTP do ouvinte.

   É apresentada uma mensagem semelhante ao seguinte texto:

```
ff64878c tcp        0      0  *.25    *.*    LISTEN.
```

7. De algum outro host, abra uma sessão Telnet com a porta SMTP do host de e-mail:

   telnet *mailhost* 25

   É apresentada uma mensagem semelhante ao seguinte texto:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. No prompt do telnet, verifique se uma mensagem pode ser retransmitida do host de e-mail:

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` é o nome de domínio da sua rede.

   Se um erro for retornado dizendo que a retransmissão é negada, a retransmissão não será ativada no host de e-mail. Contacte o administrador do sistema.

9. No prompt do telnet, envie uma mensagem de teste:

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   Certifique-se de inserir o último período (.) em uma linha por si só. O período indica ao host de e-mail que a mensagem está concluída.

   Se um erro for retornado, seu host de e-mail não será configurado corretamente. Contacte o administrador do sistema.

10. Na interface de linha de comando do ONTAP, envie uma mensagem de teste do AutoSupport para um endereço de e-mail confiável ao qual você tenha acesso:

    system node autosupport invoke -node local -type test

11. Localize o número de sequência da tentativa:

    system node autosupport history show -node local -destination smtp

    Encontre o número da sequência para a sua tentativa com base no carimbo de data/hora. É provavelmente a tentativa mais recente.

12. Exibir o erro para a tentativa de mensagem de teste:

    system node autosupport history show -node local -seq-num seq_num -fields error

    Se o erro exibido for `Login denied`, o servidor SMTP não aceita solicitações de envio do LIF de gerenciamento de cluster. Se não pretender alterar para utilizar HTTPS como protocolo de transporte, contacte o administrador de rede do site para configurar os gateways SMTP para resolver este problema.

    Se este teste for bem-sucedido, mas a mesma mensagem enviada para mailto:AutoSupport em NetApp.com não, certifique-se de que o reencaminhamento SMTP esteja ativado em todos os seus hosts de email SMTP ou use HTTPS como um protocolo de transporte.

    Se mesmo a mensagem para a conta de e-mail administrada localmente não for bem-sucedida, confirme se seus servidores SMTP estão configurados para encaminhar anexos com ambas as caraterísticas:

    - O sufixo "'7z"
    - O tipo MIME "'application/x-7x-Compressed".

Solucionar problemas do subsistema AutoSupport

Os `system node check show` comandos podem ser usados para verificar e solucionar problemas relacionados à configuração e entrega do AutoSupport.

Passo

1. Use os comandos a seguir para exibir o status do subsistema AutoSupport.

Use este comando…	Para fazer isso…
`system node autosupport check show`	Exiba o status geral do subsistema AutoSupport, como o status do destino HTTP ou HTTPS do AutoSupport, destinos SMTP do AutoSupport, servidor OnDemand do AutoSupport e configuração do AutoSupport
`system node autosupport check show-details`	Exibir o status detalhado do subsistema AutoSupport, como descrições detalhadas de erros e ações corretivas

Monitoramento de integridade

Monitore a integridade da visão geral do sistema

Os monitores de integridade monitoram proativamente certas condições críticas no cluster e emitem alertas se detetarem uma falha ou risco. Se existirem alertas ativos, o estado de funcionamento do sistema comunica um estado degradado para o cluster. Os alertas incluem as informações de que você precisa para responder à integridade degradada do sistema.

Se o estado estiver degradado, pode visualizar detalhes sobre o problema, incluindo a causa provável e as ações de recuperação recomendadas. Depois de resolver o problema, o estado de funcionamento do sistema regressa automaticamente a OK.

O status de integridade do sistema reflete vários monitores de integridade separados. Um status degradado em um monitor de integridade individual causa um status degradado para a integridade geral do sistema.

Para obter detalhes sobre como o ONTAP suporta switches de cluster para monitoramento de integridade do sistema em seu cluster, consulte *Hardware Universe*.

"Switches suportados no Hardware Universe"

Para obter detalhes sobre as causas das mensagens do AutoSupport do Monitor de integridade do comutador de cluster (CSHM) e as ações necessárias para resolver esses alertas, consulte o artigo da base de conhecimento.

"Mensagem do AutoSupport: Processo do monitor de saúde CSHM"

Como funciona o monitoramento de saúde

Os monitores de saúde individuais têm um conjunto de políticas que acionam alertas quando ocorrem determinadas condições. Entender como funciona o monitoramento de saúde pode ajudá-lo a responder a problemas e controlar futuros alertas.

O monitoramento de integridade consiste nos seguintes componentes:

- Monitores de saúde individuais para subsistemas específicos, cada um dos quais tem seu próprio estado de saúde

  Por exemplo, o subsistema Storage tem um monitor de integridade da conetividade de nó.

- Um monitor geral de integridade do sistema que consolida o estado de saúde dos monitores de saúde individuais

  Um status degradado em qualquer subsistema resulta em um status degradado para todo o sistema. Se nenhum subsistema tiver alertas, o status geral do sistema é OK.

Cada monitor de saúde é composto pelos seguintes elementos-chave:

- Alerta de que o monitor de integridade pode potencialmente aumentar

  Cada alerta tem uma definição, que inclui detalhes como a gravidade do alerta e sua causa provável.

- Políticas de saúde que identificam quando cada alerta é acionado

  Cada política de saúde tem uma expressão de regra, que é a condição ou mudança exata que aciona o alerta.

Um monitor de integridade monitora e valida continuamente os recursos em seu subsistema para mudanças de condição ou estado. Quando uma condição ou mudança de estado corresponde a uma expressão de regra em uma política de saúde, o monitor de integridade gera um alerta. Um alerta faz com que o estado de funcionamento do subsistema e o estado geral do estado do sistema se degradem.

Maneiras de responder a alertas de integridade do sistema

Quando um alerta de integridade do sistema ocorre, você pode reconhecê-lo, saber mais sobre ele, reparar a condição subjacente e impedir que ele ocorra novamente.

Quando um monitor de saúde gera um alerta, você pode responder de qualquer uma das seguintes maneiras:

- Obtenha informações sobre o alerta, que inclui o recurso afetado, a gravidade do alerta, a causa provável, o possível efeito e as ações corretivas.
- Obtenha informações detalhadas sobre o alerta, como a hora em que o alerta foi gerado e se alguém já reconheceu o alerta.
- Obtenha informações relacionadas à integridade sobre o estado do recurso ou subsistema afetado, como um compartimento ou disco específico.
- Reconheça o alerta para indicar que alguém está trabalhando no problema e identifique-se como o ""reconhecimento"".
- Resolva o problema tomando as ações corretivas fornecidas no alerta, como a fixação de cabeamento para resolver um problema de conetividade.
- Exclua o alerta, se o sistema não o apagou automaticamente.
- Suprimir um alerta para impedir que ele afete o status de integridade de um subsistema.

  Suprimir é útil quando você entende um problema. Depois de suprimir um alerta, ele ainda pode ocorrer, mas a integridade do subsistema é exibida como "'ok-with-suppressed.'" quando o alerta suprimido ocorre.

Personalização do alerta de integridade do sistema

Você pode controlar quais alertas um monitor de integridade gera ativando e desativando as políticas de integridade do sistema que definem quando os alertas são acionados. Isso permite que você personalize o sistema de monitoramento de integridade para seu ambiente específico.

Você pode aprender o nome de uma política exibindo informações detalhadas sobre um alerta gerado ou exibindo definições de política para um monitor de integridade específico, nó ou ID de alerta.

Desativar políticas de saúde é diferente de suprimir alertas. Quando você suprime um alerta, ele não afeta o status de integridade do subsistema, mas o alerta ainda pode ocorrer.

Se você desabilitar uma política, a condição ou estado definido em sua expressão de regra de política não acionará mais um alerta.

Exemplo de um alerta que você deseja desativar

Por exemplo, suponha que ocorra um alerta que não seja útil para você. Você usa o `system health alert show -instance` comando para obter o ID da política para o alerta. Você usa o ID da política no `system health policy definition show` comando para exibir informações sobre a política. Depois de analisar a expressão da regra e outras informações sobre a política, você decide desativar a política. Você usa o `system health policy definition modify` comando para desativar a política.

Como os alertas de saúde acionam mensagens e eventos do AutoSupport

Os alertas de integridade do sistema acionam mensagens e eventos AutoSupport no

sistema de Gestão de Eventos (EMS), permitindo-lhe monitorizar a integridade do sistema utilizando mensagens AutoSupport e o EMS, além de utilizar diretamente o sistema de monitorização de integridade.

O sistema envia uma mensagem AutoSupport dentro de cinco minutos após um alerta. A mensagem AutoSupport inclui todos os alertas gerados desde a mensagem AutoSupport anterior, exceto para alertas que duplicam um alerta para o mesmo recurso e causa provável na semana anterior.

Alguns alertas não acionam mensagens AutoSupport. Um alerta não aciona uma mensagem AutoSupport se a sua política de integridade desativar o envio de mensagens AutoSupport. Por exemplo, uma política de integridade pode desativar as mensagens do AutoSupport por padrão porque o AutoSupport já gera uma mensagem quando o problema ocorre. Você pode configurar políticas para não acionar mensagens AutoSupport usando o `system health policy definition modify` comando.

Você pode ver uma lista de todas as mensagens AutoSupport acionadas por alerta enviadas na semana anterior usando o `system health autosupport trigger history show` comando.

Os alertas também acionam a geração de eventos para o EMS. Um evento é gerado cada vez que um alerta é criado e cada vez que um alerta é apagado.

Monitores de integridade do cluster disponíveis

Existem vários monitores de integridade que monitorizam diferentes partes de um cluster. Os monitores de integridade ajudam você a se recuperar de erros nos sistemas ONTAP detetando eventos, enviando alertas para você e excluindo eventos conforme eles forem claros.

Nome do monitor de integridade (identificador)	Nome do subsistema (identificador)	Finalidade
Interrutor do cluster (interrutor do cluster)	Interrutor (estado do interrutor)	Monitora os switches de rede de cluster e os switches de rede de gerenciamento para temperatura, utilização, configuração de interface, redundância (somente switches de rede de cluster) e operação de ventilador e fonte de alimentação. O monitor de integridade do comutador de cluster comunica com os comutadores através do SNMP. SNMPv2c é a configuração padrão. A partir do ONTAP 9.2, este monitor pode detetar e reportar quando uma central de cluster foi reinicializada desde o último período de polling.
MetroCluster Fabric	Interrutor	Monitora a topologia da malha de back-end de configuração do MetroCluster e deteta configurações incorretas, como cabeamento e zoneamento incorretos e falhas de ISL.
MetroCluster Saúde	Interconexão, RAID e armazenamento	Monitora os adaptadores FC-VI, os adaptadores iniciador FC, os discos e agregados esquerdos e as portas entre clusters
Conetividade do nó (nó-conexão)	Operações ininterruptas de CIFS (CIFS-NDO)	Monitora conexões SMB para operações ininterruptas com aplicações Hyper-V.
Storage (conexão SAS)	Monitora compartimentos, discos e adaptadores no nível do nó para ver os caminhos e as conexões apropriados.	Sistema
não aplicável	Agrega informações de outros monitores de saúde.	Conetividade do sistema (conexão do sistema)

Receba alertas de integridade do sistema automaticamente

Você pode visualizar manualmente os alertas de integridade do sistema usando o `system health alert show` comando. No entanto, você deve assinar mensagens específicas do sistema de Gerenciamento de Eventos (EMS) para receber notificações automaticamente quando um monitor de integridade gera um alerta.

Sobre esta tarefa

O procedimento a seguir mostra como configurar notificações para todas as mensagens hm.alert.raised e todas as mensagens hm.alert.cleared.

Todas as mensagens hm.alert.raised e todas as mensagens hm.alert.cleared incluem um trap SNMP. Os nomes dos traps SNMP são `HealthMonitorAlertRaised` e `HealthMonitorAlertCleared`. Para obter informações sobre traps SNMP, consulte o *Network Management Guide*.

Passos

1. Utilize o `event destination create` comando para definir o destino para o qual pretende enviar as mensagens EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilize o `event route add-destinations` comando para encaminhar a `hm.alert.raised` mensagem e a `hm.alert.cleared` mensagem para um destino.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Informações relacionadas

"Gerenciamento de rede"

Responder à integridade do sistema degradado

Quando o estado de funcionamento do sistema estiver degradado, pode apresentar alertas, ler sobre a causa provável e as acões correctivas, apresentar informações sobre o subsistema degradado e resolver o problema. Alertas suprimidos também são mostrados para que você possa modificá-los e ver se eles foram reconhecidos.

Sobre esta tarefa

Você pode descobrir que um alerta foi gerado visualizando uma mensagem AutoSupport ou um evento EMS, ou usando os `system health` comandos.

Passos

1. Use o `system health alert show` comando para visualizar os alertas que estão comprometendo a integridade do sistema.
2. Leia a causa provável, o possível efeito e as ações corretivas do alerta para determinar se você pode

resolver o problema ou precisa de mais informações.

3. Se você precisar de mais informações, use o `system health alert show -instance` comando para exibir informações adicionais disponíveis para o alerta.
4. Use o `system health alert modify` comando com o `-acknowledge` parâmetro para indicar que você está trabalhando em um alerta específico.
5. Tome medidas corretivas para resolver o problema conforme descrito pelo `Corrective Actions` campo no alerta.

   As ações corretivas podem incluir a reinicialização do sistema.

   Quando o problema é resolvido, o alerta é automaticamente apagado. Se o subsistema não tiver outros alertas, a integridade do subsistema será alterada para `OK`. Se a integridade de todos os subsistemas estiver OK, o estado geral do sistema muda para `OK`.

6. Utilize o `system health status show` comando para confirmar se o estado de funcionamento do sistema é `OK`.

   Se o estado de funcionamento do sistema não for `OK` , repita este procedimento.

Exemplo de resposta à integridade do sistema degradado

Ao analisar um exemplo específico de integridade do sistema degradado causado por um compartimento que não tem dois caminhos para um nó, você pode ver o que a CLI exibe quando você responde a um alerta.

Depois de iniciar o ONTAP, você verifica a integridade do sistema e descobre que o status está degradado:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Você mostra alertas para descobrir onde está o problema e vê que o compartimento 2 não tem dois caminhos para o node1:

```
      cluster1::>system health alert show
                Node: node1
            Resource: Shelf ID 2
            Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

Você exibe detalhes sobre o alerta para obter mais informações, incluindo o ID de alerta:

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

Você reconhece o alerta para indicar que está trabalhando nele.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Você conserta o cabeamento entre as prateleiras 2 e node1 e reinicializa o sistema. Em seguida, você verifica novamente a integridade do sistema e vê se o status é `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Configurar a descoberta de switches de rede de gerenciamento e cluster

O monitor de integridade do switch de cluster tenta automaticamente descobrir os switches de rede de gerenciamento e cluster usando o Protocolo de detecção de Cisco (CDP). Você deve configurar o monitor de integridade se ele não conseguir descobrir automaticamente um switch ou se você não quiser usar o CDP para deteção automática.

Sobre esta tarefa

O `system cluster-switch show` comando lista os switches que o monitor de integridade descobriu. Se você não vir um switch que você esperava ver nessa lista, o monitor de integridade não poderá descobri-lo automaticamente.

Passos

1. Se você quiser usar o CDP para deteção automática, faça o seguinte:

   a. Certifique-se de que o Protocolo de detecção de Cisco (CDP) está ativado nos seus comutadores.

      Consulte a documentação do switch para obter instruções.

   b. Execute o seguinte comando em cada nó no cluster para verificar se o CDP está ativado ou desativado:

      `run -node *node_name* -command options cdpd.enable`

      Se o CDP estiver ativado, passe à operação d. se o CDP estiver desativado, passe à operação c.

   c. Execute o seguinte comando para ativar o CDP:

      `run -node *node_name* -command options cdpd.enable on`

   Aguarde cinco minutos antes de ir para o próximo passo.

   a. Use o `system cluster-switch show` comando para verificar se o ONTAP agora pode descobrir automaticamente os switches.

2. Se o monitor de integridade não conseguir descobrir automaticamente um switch, use o `system cluster-switch create` comando para configurar a descoberta do switch:

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Aguarde cinco minutos antes de ir para o próximo passo.

3. Use o `system cluster-switch show` comando para verificar se o ONTAP pode descobrir o switch para o qual você adicionou informações.

Depois de terminar

Verifique se o monitor de integridade pode monitorar seus switches.

Verifique o monitoramento dos switches de rede de gerenciamento e cluster

O monitor de integridade do switch de cluster tenta monitorar automaticamente os switches que ele descobre; no entanto, o monitoramento pode não acontecer automaticamente se os switches não estiverem configurados corretamente. Você deve verificar se o monitor de integridade está configurado corretamente para monitorar seus switches.

Passos

1. Para identificar os switches detetados pelo monitor de integridade do switch de cluster, digite o seguinte comando:

   ONTAP 9 F.8 e mais tarde

   `system switch ethernet show`

   ONTAP 9 F.7 e anteriores

   `system cluster-switch show`

   Se a `Model` coluna exibir o valor `OTHER`, o ONTAP não poderá monitorar o switch. O ONTAP define o valor para `OTHER` se um switch que ele descobre automaticamente não for suportado para monitoramento de integridade.

   Se um switch não for exibido na saída do comando, você deverá configurar a descoberta do switch.

2. Atualize para o software de switch suportado mais recente e consulte o arquivo de configuração (RCF) no site de suporte da NetApp.

   "Página de transferências do suporte da NetApp"

   A cadeia de carateres da comunidade no RCF do switch deve corresponder à cadeia de carateres da comunidade que o monitor de integridade está configurado para usar. Por padrão, o monitor de integridade usa a cadeia de carateres da comunidade `cshm1!` .

   Neste momento, o monitor de integridade só suporta SNMPv2.

   Se você precisar alterar informações sobre um switch que o cluster monitora, você poderá modificar a cadeia de carateres da comunidade usada pelo monitor de integridade usando o seguinte comando:

ONTAP 9 F.8 e mais tarde

```
system switch ethernet modify
```

ONTAP 9 F.7 e anteriores

```
system cluster-switch modify
```

3. Verifique se a porta de gerenciamento do switch está conetada à rede de gerenciamento.

   Esta conexão é necessária para executar consultas SNMP.

Comandos para monitorar a integridade do seu sistema

Você pode usar os `system health` comandos para exibir informações sobre a integridade dos recursos do sistema, responder a alertas e configurar alertas futuros. O uso dos comandos CLI permite exibir informações detalhadas sobre como o monitoramento de integridade é configurado. As páginas man para os comandos contêm mais informações.

Apresentar o estado da integridade do sistema

Se você quiser…	Use este comando…
Apresentar o estado de funcionamento do sistema, que reflete o estado geral dos monitores de saúde individuais	`system health status show`
Apresentar o estado de funcionamento dos subsistemas para os quais a monitorização de integridade está disponível	`system health subsystem show`

Exibir o status da conetividade do nó

Se você quiser…	Use este comando…
Exiba detalhes sobre a conectividade do nó para o compartimento de storage, incluindo informações de porta, velocidade da porta HBA, taxa de transferência de e/S e taxa de operações de e/S por segundo	`storage shelf show -connectivity` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada prateleira.
Exiba informações sobre unidades e LUNs de storage, incluindo o espaço utilizável, os números de compartimento e compartimento e o nome do nó proprietário	`storage disk show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada unidade.

Se você quiser…	Use este comando…
Exiba informações detalhadas sobre as portas do compartimento de armazenamento, incluindo o tipo, a velocidade e o status da porta	`storage port show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada adaptador.

Gerenciar a descoberta de switches de rede de cluster, armazenamento e gerenciamento

Se você quiser…	Use este comando. (ONTAP 9.8 e posterior)	Use este comando. (ONTAP 9 .7 e anteriores)
Apresentar os interrutores que o grupo de instrumentos monitoriza	`system switch ethernet show`	`system cluster-switch show`
Exiba os switches que o cluster monitora atualmente, incluindo os switches que você excluiu (mostrados na coluna motivo na saída do comando) e as informações de configuração necessárias para acesso à rede ao cluster e aos switches de rede de gerenciamento. Este comando está disponível no nível de privilégio avançado.	`system switch ethernet show-all`	`system cluster-switch show-all`
Configurar a descoberta de um switch não descoberto	`system switch ethernet create`	`system cluster-switch create`
Modificar informações sobre um switch que o cluster monitora (por exemplo, nome do dispositivo, endereço IP, versão SNMP e cadeia de carateres da comunidade)	`system switch ethernet modify`	`system cluster-switch modify`
Desativar a monitorização de um interrutor	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Desative a descoberta e o monitoramento de um switch e exclua as informações de configuração do switch	`system switch ethernet delete`	`system cluster-switch delete`

Se você quiser…	Use este comando. (ONTAP 9.8 e posterior)	Use este comando. (ONTAP 9 .7 e anteriores)
Remover permanentemente as informações de configuração do switch que são armazenadas no banco de dados (isso rehabilita a descoberta automática do switch)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Ative o registo automático para enviar com mensagens AutoSupport.	`system switch ethernet log`	`system cluster-switch log`

Responder a alertas gerados

Se você quiser…	Use este comando…
Exiba informações sobre alertas gerados, como o recurso e o nó em que o alerta foi acionado, e a gravidade e a causa provável do alerta	`system health alert show`
Exibir informações sobre cada alerta gerado	`system health alert show -instance`
Indique que alguém está trabalhando em um alerta	`system health alert modify`
Confirme um alerta	`system health alert modify -acknowledge`
Suprimir um alerta subsequente para que não afete o estado de funcionamento de um subsistema	`system health alert modify -suppress`
Exclua um alerta que não foi apagado automaticamente	`system health alert delete`
Exiba informações sobre as mensagens do AutoSupport que alertas dispararam na última semana, por exemplo, para determinar se um alerta acionou uma mensagem do AutoSupport	`system health autosupport trigger history show`

Configurar alertas futuros

Se você quiser…	Use este comando…
Ative ou desative a política que controla se um estado de recurso específico gera um alerta específico	`system health policy definition modify`

Exiba informações sobre como o monitoramento de integridade é configurado

Se você quiser…	Use este comando…
Exibir informações sobre monitores de integridade, como seus nós, nomes, subsistemas e status	`system health config show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada monitor de integridade.
Exiba informações sobre os alertas que um monitor de integridade pode gerar	`system health alert definition show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada definição de alerta.
Exiba informações sobre as políticas do monitor de integridade, que determinam quando os alertas são gerados	`system health policy definition show` Use o `-instance` parâmetro para exibir informações detalhadas sobre cada política. Use outros parâmetros para filtrar a lista de alertas - por exemplo, por status da política (habilitado ou não), monitor de integridade, alerta e assim por diante.

Apresentar informações ambientais

Os sensores ajudam a monitorar os componentes ambientais do seu sistema. As informações que você pode exibir sobre os sensores ambientais incluem seus avisos de tipo, nome, estado, valor e limite.

Passo

1. Para exibir informações sobre sensores ambientais, use o `system node environment sensors show` comando.

Análise do sistema de arquivos

Visão geral do File System Analytics

A análise do sistema de arquivos (FSA) foi apresentada pela primeira vez no ONTAP 9.8 para fornecer visibilidade em tempo real sobre as tendências de utilização de arquivos e capacidade de storage nos volumes ONTAP FlexGroup ou FlexVol. Essa funcionalidade nativa elimina a necessidade de ferramentas externas e fornece insights importantes sobre como seu storage é utilizado e se há oportunidades de otimizar o storage para suas necessidades empresariais.

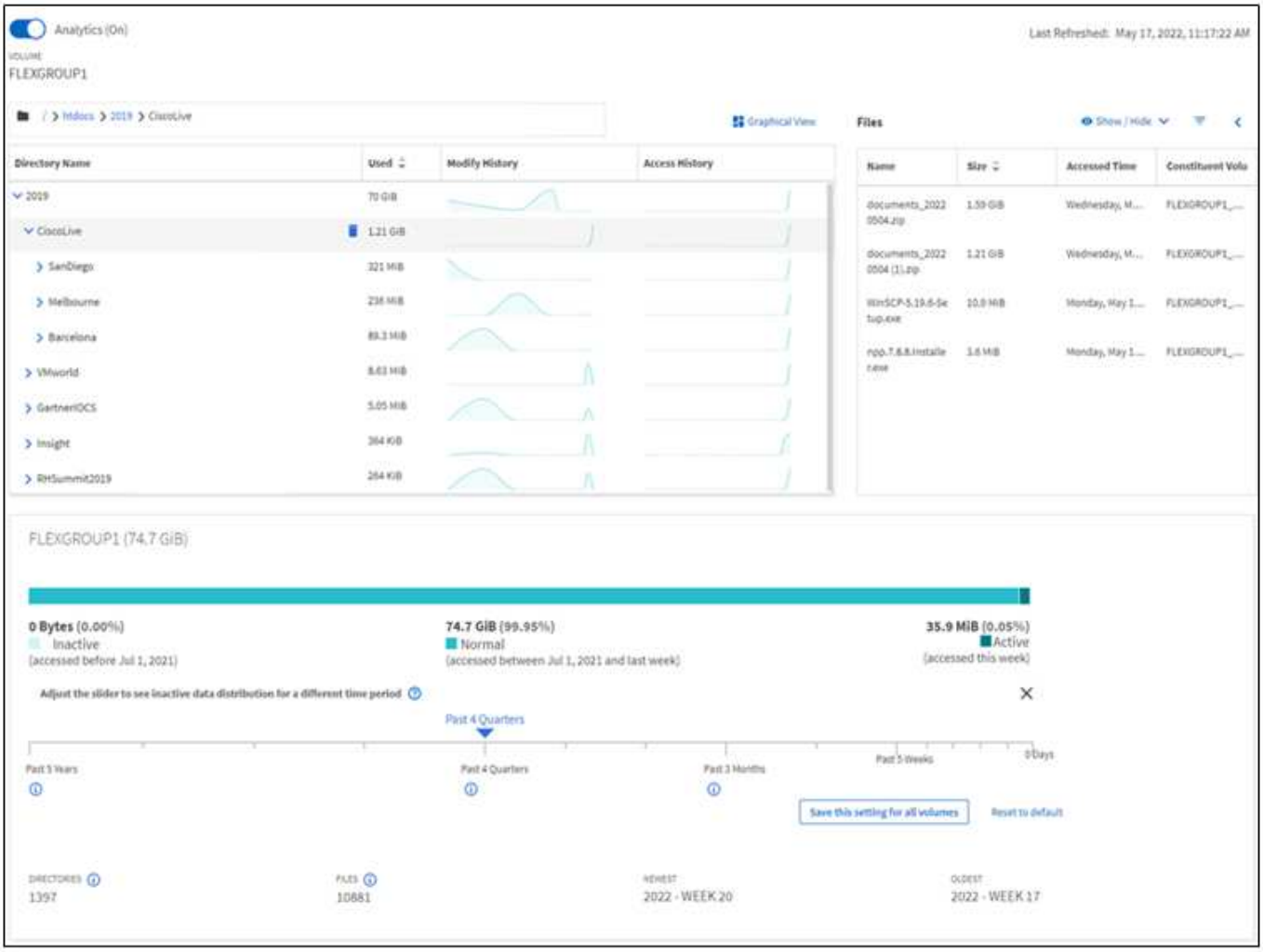
Com o FSA, você tem visibilidade em todos os níveis da hierarquia do sistema de arquivos de um volume no nas. Por exemplo, você pode obter insights de uso e capacidade nos níveis de VM de storage (SVM), volume,

diretório e arquivo. Você pode usar o FSA para responder perguntas como:

- O que está preenchendo meu armazenamento e há arquivos grandes que eu possa mover para outro local de armazenamento?
- Quais são meus volumes, diretórios e arquivos mais ativos? A performance do meu storage é otimizada para as necessidades dos meus usuários?
- Quantos dados foram adicionados no último mês?
- Quem são meus usuários de storage mais ativos ou menos ativos?
- Quantos dados inativos ou inativos estão no meu storage primário? Posso migrar esses dados para uma camada pouco econômica?
- Minhas alterações planejadas de qualidade do serviço afetarão negativamente o acesso a arquivos críticos e acessados com frequência?

A análise do sistema de arquivos está integrada ao ONTAP System Manager. As visualizações no System Manager fornecem:

- Visibilidade em tempo real para gerenciamento e operação de dados eficazes
- Coleta e agregação de dados em tempo real
- Subdiretório e tamanhos de arquivo e contagens, juntamente com perfis de desempenho associados
- Histogramas de idade de arquivo para modificar e histórico de acesso



Tipos de volume suportados

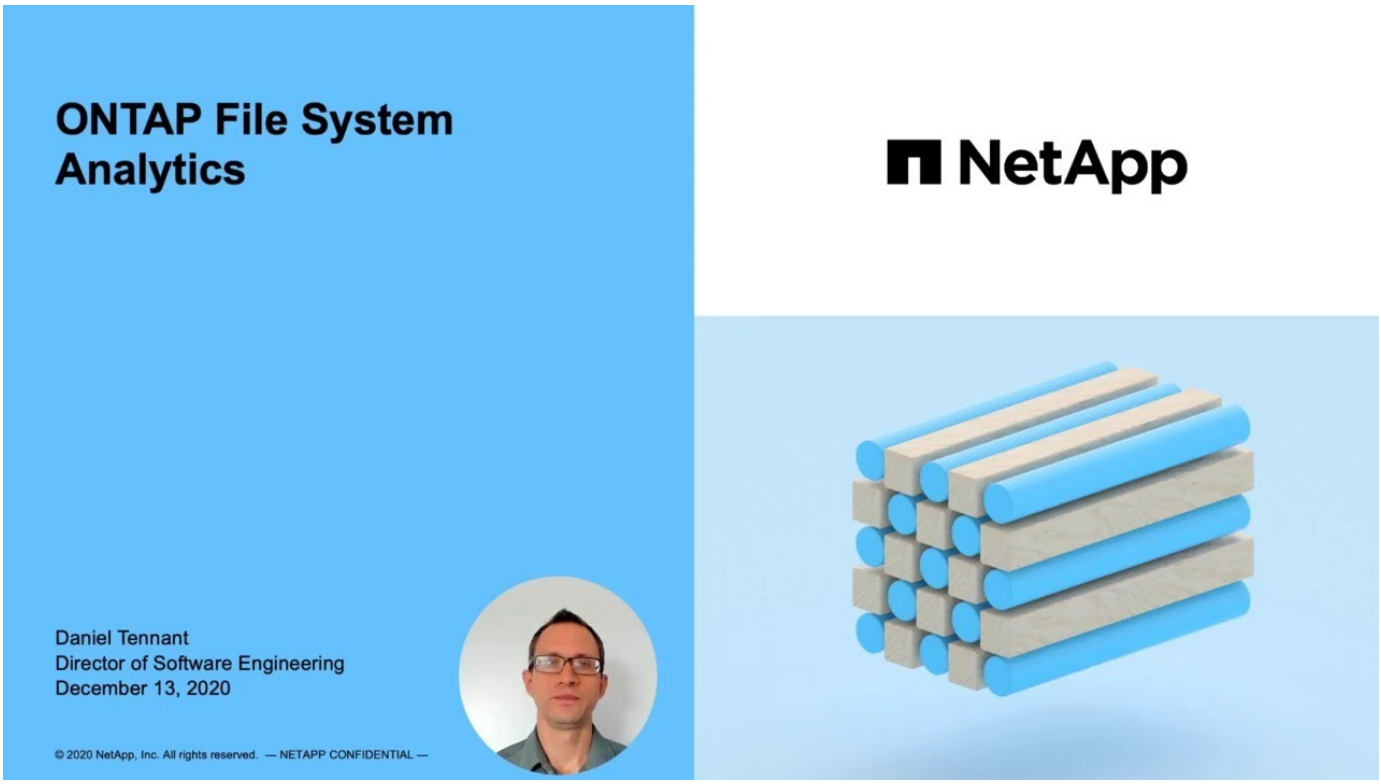
A análise do sistema de arquivos foi projetada para fornecer visibilidade em volumes com dados nas ativos, com exceção dos caches do FlexCache e dos volumes de destino do SnapMirror.

Disponibilidade do recurso análise do sistema de arquivos

Cada versão do ONTAP expande o escopo da análise do sistema de arquivos.

	ONTAP 9.15,1	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1	ONTAP 9.10,1	ONTAP 9.9,1	ONTAP 9,8
Visualização no System Manager	✓	✓	✓	✓	✓	✓	✓	✓
Análise de capacidade	✓	✓	✓	✓	✓	✓	✓	✓
Informações de dados inativos	✓	✓	✓	✓	✓	✓	✓	✓
Suporte para volumes transferidos do modo Data ONTAP 7	✓	✓	✓	✓	✓	✓	✓	
Capacidade de personalizar o período inativo no System Manager	✓	✓	✓	✓	✓	✓	✓	
Monitorização de atividade em nível de volume	✓	✓	✓	✓	✓	✓		
Faça o download dos dados de acompanhamento da atividade para CSV	✓	✓	✓	✓	✓	✓		
Monitoramento de atividades no nível da SVM	✓	✓	✓	✓	✓			
Linha do tempo	✓	✓	✓	✓	✓			
Análise de utilização	✓	✓	✓	✓				
Opção para ativar a análise do sistema de ficheiros por predefinição	✓	✓	✓					
Inicialização do monitor de progresso da digitalização	✓	✓						

Saiba mais sobre o File System Analytics



Leitura adicional

- "TR 4687: Diretrizes de práticas recomendadas para análise do sistema de arquivos do ONTAP"
- "Base de Conhecimento: Latência alta ou flutuante após ativar a análise do sistema de arquivos do NetApp ONTAP"

Ative a análise do sistema de ficheiros

Para coletar e exibir dados de uso, como análise de capacidade, você precisa ativar o File System Analytics em um volume.

Sobre esta tarefa

- A partir do ONTAP 9.8, você pode ativar a análise do sistema de arquivos em um volume novo ou existente. Se você atualizar um sistema para o ONTAP 9.8 ou posterior, certifique-se de que todos os processos de atualização foram concluídos antes de ativar a análise do sistema de arquivos.
- O tempo necessário para habilitar a análise depende do tamanho e do conteúdo do volume. O System Manager exibe o progresso e apresenta dados analíticos quando concluído. Se precisar de informações mais precisas sobre o progresso da digitalização de inicialização, você pode usar o comando ONTAP CLI `volume analytics show`.
  - A partir do ONTAP 9.14,1, o ONTAP fornece o acompanhamento do progresso para a verificação de inicialização, além de notificações sobre eventos de limitação que afetam o progresso da digitalização.
  - A partir do ONTAP 9.15,1, você pode realizar apenas quatro verificações de inicialização simultaneamente em um nó. Tem de esperar que uma digitalização seja concluída antes de iniciar uma nova digitalização. O ONTAP também impõe que haja espaço disponível suficiente no volume e apresenta uma mensagem de erro se não houver. Certifique-se de que pelo menos 5 a 8% do espaço disponível do volume esteja livre. Se o volume tiver o dimensionamento automático ativado, calcule o tamanho disponível com base no tamanho máximo do crescimento automático.
  - Para mais considerações relacionadas com a digitalização de inicialização, Considerações de

digitalizaçãoconsulte .

Ative a análise do sistema de arquivos em um volume existente

Você pode ativar a análise do sistema de arquivos com o ONTAP System Manager ou a CLI.

Exemplo 36. Passo

System Manager

Em ONTAP 9 .8 e 9.9.1	Começando em ONTAP 9.10,1
1. Selecione **armazenamento > volumes**. 2. Selecione o volume desejado e, em seguida, selecione **Explorer**. 3. Selecione **Ativar o Analytics** ou **Desativar o Analytics**.	1. Selecione **armazenamento > volumes**. 2. Selecione o volume pretendido. No menu volume individual, selecione **sistema de ficheiros > Explorador**. 3. Selecione **Ativar o Analytics** ou **Desativar o Analytics**.

CLI

Ative a análise do sistema de arquivos com a CLI

1. Execute o seguinte comando:
`volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]` Por padrão, o comando é executado em primeiro plano; o ONTAP exibe o progresso e apresenta dados analíticos quando concluído. Se você precisar de informações mais precisas, você pode executar o comando em segundo plano usando a `-foreground false` opção e, em seguida, usar o `volume analytics show` comando para exibir o progresso de inicialização na CLI.
2. Depois de habilitar com êxito a análise do sistema de arquivos, use o Gerenciador do sistema ou a API REST do ONTAP para exibir os dados analíticos.

Modifique as configurações padrão de análise do sistema de arquivos

A partir do ONTAP 9.13,1, é possível modificar as configurações de SVM ou clusters para habilitar a análise do sistema de arquivos por padrão em novos volumes.

Exemplo 37. Passos

System Manager

Se você estiver usando o System Manager, poderá modificar as configurações de VM ou cluster de armazenamento para habilitar a análise de capacidade e o acompanhamento de atividades na criação de volume por padrão. A habilitação padrão se aplica somente a volumes criados após a modificação das configurações, não a volumes existentes.

Modificar as configurações de análise do sistema de arquivos em um cluster

1. No System Manager, navegue até **Configurações de cluster**.
2. Em **Configurações de cluster**, consulte a guia Configurações do sistema de arquivos. Para modificar as definições, selecione o ícone.
3. No campo **Rastreamento de atividade**, insira os nomes dos SVMs para habilitar o Rastreamento de atividades por padrão. Deixar o campo em branco deixará o acompanhamento de atividades desativado em todos os SVMs.

   Desmarque a caixa **Ativar em novas VMs de armazenamento** para desativar o acompanhamento de atividades por padrão em novas VMs de armazenamento.

4. No campo **Analytics**, insira os nomes das VMs de armazenamento para as quais você deseja que a análise de capacidade esteja habilitada por padrão. Deixar o campo em branco deixará a análise de capacidade desativada em todos os SVMs.

   Desmarque a caixa **Ativar em novas VMs de armazenamento** para desativar a análise de capacidade por padrão em novas VMs de armazenamento.

5. Selecione **Guardar**.

Modificar as configurações de análise do sistema de arquivos em uma SVM

1. Selecione o SVM que você deseja modificar e, em seguida, **Storage VM settings**.
2. No cartão **File System Analytics**, use as alternâncias para ativar ou desativar o acompanhamento de atividades e a análise de capacidade para todos os novos volumes na VM de armazenamento.

CLI

Você pode configurar a VM de storage para habilitar a análise do sistema de arquivos por padrão em novos volumes usando a CLI do ONTAP.

Por padrão, ative a análise do sistema de arquivos em uma SVM

1. Modifique o SVM para habilitar a análise de capacidade e o acompanhamento de atividades por padrão em todos os volumes recém-criados:
   `vserver modify -vserver` *`svm_name`* `-auto-enable-activity-tracking true -auto -enable-analytics true`

Exibir atividade do sistema de arquivos

Depois que o File System Analytics (FSA) estiver ativado, você poderá visualizar o conteúdo do diretório raiz de um volume selecionado, classificado pelo espaço usado em cada subárvore.

Selecione qualquer objeto de sistema de arquivos para navegar no sistema de arquivos e exibir informações

detalhadas sobre cada objeto em um diretório. Informações sobre diretórios também podem ser exibidas graficamente. Ao longo do tempo, os dados históricos são exibidos para cada subárvore. O espaço usado não é classificado se houver mais de 3000 diretórios.

Explorador

A tela File System Analytics **Explorer** consiste em três áreas:

- Exibição em árvore de diretórios e subdiretórios; lista expansível mostrando nome, tamanho, histórico de modificação e histórico de acesso.
- Arquivos; mostrando nome, tamanho e tempo acessado para o objeto selecionado na lista de diretórios.
- Comparação de dados ativos e inativos para o objeto selecionado na lista de diretórios.

  Começando com ONTAP 9.9,1, você pode personalizar o intervalo a ser relatado. O valor padrão é um ano. Com base nessas personalizações, você pode tomar medidas corretivas, como mover volumes e modificar a política de disposição em categorias.

A hora acessada é mostrada por padrão. No entanto, se o padrão de volume tiver sido alterado a partir da CLI (definindo a `-atime-update` opção como `false` com o `volume modify` comando), então somente o último tempo modificado será mostrado. Por exemplo:

- A exibição em árvore não exibirá o **histórico de acesso**.
- A vista de ficheiros será alterada.
- A vista de dados ativo/inativo será baseada no tempo modificado (`mtime`).

Usando esses monitores, você pode examinar o seguinte:

- Localizações do sistema de arquivos que consomem mais espaço
- Informações detalhadas sobre uma árvore de diretórios, incluindo contagem de arquivos e subdiretórios dentro de diretórios e subdiretórios
- Locais do sistema de arquivos que contêm dados antigos (por exemplo, árvores de arranhão, temperatura ou log)

Tenha em mente os seguintes pontos ao interpretar a saída FSA:

- A FSA mostra onde e quando seus dados estão em uso, não quantos dados estão sendo processados. Por exemplo, o grande consumo de espaço por arquivos recentemente acessados ou modificados não indica necessariamente altas cargas de processamento do sistema.
- A forma como o separador **Explorador de volumes** calcula o consumo de espaço para o FSA pode ser diferente de outras ferramentas. Em particular, pode haver diferenças significativas em comparação com o consumo relatado no **volume Overview** se o volume tiver recursos de eficiência de armazenamento ativados. Isso ocorre porque a guia **Explorador de volumes** não inclui economia de eficiência.
- Devido às limitações de espaço na exibição do diretório, não é possível visualizar uma profundidade de diretório superior a 8 níveis na *Vista de lista*. Para visualizar diretórios com mais de 8 níveis de profundidade, você deve alternar para *Vista gráfica*, localizar o diretório desejado e, em seguida, voltar para *Vista de lista*. Isto permitirá espaço adicional no ecrã.

Passos

1. Exibir o conteúdo do diretório raiz de um volume selecionado:

Em ONTAP 9 .8 e 9.9.1	Começando em ONTAP 9.10,1
Clique em **armazenamento > volumes**, selecione o volume desejado e clique em **Explorer**.	Selecione **armazenamento > volumes** e selecione o volume desejado. No menu volume individual, selecione **sistema de ficheiros > Explorador**.

Ative o acompanhamento de atividades

A partir do ONTAP 9.10,1, a análise do sistema de arquivos inclui um recurso de acompanhamento de atividades que permite identificar objetos ativos e fazer o download dos dados como um arquivo CSV. A partir do ONTAP 9.11,1, o acompanhamento de atividades é expandido para o escopo da SVM. Também começando no ONTAP 9.11,1, o Gerenciador de sistema apresenta uma linha do tempo para o acompanhamento de atividades, permitindo que você analise até cinco minutos de dados de acompanhamento de atividades.

O acompanhamento de atividades permite a monitorização em quatro categorias:

- Diretórios
- Ficheiros
- Clientes
- Usuários

Para cada categoria monitorada, o acompanhamento de atividades exibirá IOPs de leitura, escrita IOPs, leitura de throughput e gravação de throughput. As consultas sobre o acompanhamento de atividades são atualizadas a cada 10 a 15 segundos referentes aos pontos quentes vistos no sistema em relação ao intervalo de cinco segundos anterior.

As informações de rastreamento de atividade são aproximadas e a precisão dos dados depende da distribuição do tráfego de e/S de entrada.

Ao visualizar o acompanhamento de atividades no System Manager no nível do volume, apenas o menu do volume expandido será atualizado ativamente. Se a visualização de quaisquer volumes estiver colapsada, eles não serão atualizados até que a exibição do volume seja expandida. Você pode parar as atualizações com o botão **Pausa Atualizar**. Os dados de atividade podem ser baixados em um formato CSV que exibirá todos os dados pontuais capturados para o volume selecionado.

Com o recurso de linha do tempo disponível a partir do ONTAP 9.11,1, você pode manter um Registro da atividade de hotspot em um volume ou SVM, atualizando continuamente aproximadamente a cada cinco segundos e mantendo os cinco minutos de dados anteriores. Os dados da linha do tempo são retidos apenas para campos que são área visível da página. Se você recolher uma categoria de rastreamento ou rolar para que a linha do tempo esteja fora de exibição, a linha do tempo deixará de coletar dados. Por padrão, os cronogramas são desativados e serão automaticamente desativados quando você navegar para fora da guia atividade.

Ative o acompanhamento de atividades para um único volume

Você pode ativar o acompanhamento de atividades com o Gerenciador de sistema do ONTAP ou com a CLI.

Sobre esta tarefa

Se você usar o RBAC com a API REST do ONTAP ou o Gerenciador de sistemas, precisará criar funções

personalizadas para gerenciar o acesso ao acompanhamento de atividades. Consulte Controles de acesso baseados em função para obter este processo.

System Manager

Passos

1. Selecione **armazenamento > volumes**. Selecione o volume pretendido. No menu volume individual, selecione sistema de arquivos e, em seguida, selecione a guia atividade.
2. Certifique-se de que **Activity Tracking** esteja ativado para visualizar relatórios individuais em diretórios, arquivos, clientes e usuários superiores.
3. Para analisar dados em maior profundidade sem atualizações, selecione **Pausa Atualizar**. Você pode baixar os dados para ter um Registro CSV do relatório também.

CLI

Passos

1. Ativar monitorização de atividade:

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. Verifique se o estado de monitorização de atividade para um volume está ligado ou desligado com o comando:

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. Uma vez ativado, use o Gerenciador de sistema do ONTAP ou a API REST do ONTAP para exibir dados de acompanhamento de atividades.

Ative o acompanhamento de atividades para vários volumes

Você pode ativar o acompanhamento de atividades para vários volumes com o System Manager ou a CLI.

Sobre esta tarefa

Se você usar o RBAC com a API REST do ONTAP ou o Gerenciador de sistemas, precisará criar funções personalizadas para gerenciar o acesso ao acompanhamento de atividades. Consulte Controles de acesso baseados em função para obter este processo.

System Manager

Ativar para volumes específicos

1. Selecione **armazenamento > volumes**. Selecione o volume pretendido. No menu volume individual, selecione sistema de arquivos e, em seguida, selecione a guia atividade.
2. Selecione os volumes em que pretende ativar o acompanhamento de atividades. Na parte superior da lista de volume, selecione o botão **mais Opções**. Selecione **Ativar monitorização de atividade**.
3. Para exibir o acompanhamento de atividades no nível SVM, selecione o SVM específico que você gostaria de exibir em **Storage > volumes**. Navegue até a guia sistema de arquivos e, em seguida, Activity e você verá os dados dos volumes que têm o acompanhamento de atividades ativado.

Ativar para todos os volumes

1. Selecione **armazenamento > volumes**. Selecione uma SVM no menu.
2. Navegue até a guia **sistema de arquivos**, escolha a guia **mais** para ativar o acompanhamento de atividades em todos os volumes no SVM.

CLI

A partir do ONTAP 9.13,1, você pode ativar o acompanhamento de atividades para vários volumes usando a CLI do ONTAP.

Passos

1. Ativar monitorização de atividade:

   `volume activity-tracking on -vserver svm_name -volume [*|!volume_names]`

   ```
   `*`Use para ativar o acompanhamento de atividades para todos os
   volumes na VM de armazenamento especificada.
   ```

   Use `!` seguido por nomes de volume para ativar o acompanhamento de atividades para todos os volumes na SVM, exceto os volumes nomeados.

2. Confirme se a operação foi bem-sucedida:

   `volume show -fields activity-tracking-state`

3. Uma vez ativado, use o Gerenciador de sistema do ONTAP ou a API REST do ONTAP para exibir dados de acompanhamento de atividades.

Habilite a análise de uso

A partir do ONTAP 9.12,1, você pode habilitar a análise de uso para ver quais diretórios dentro de um volume estão usando mais espaço. Você pode exibir o número total de diretórios em um volume ou o número total de arquivos em um volume. Os relatórios são limitados aos diretórios 25 que usam mais espaço.

As análises para grandes diretórios são atualizadas a cada 15 minutos. Você pode monitorar a atualização mais recente verificando o carimbo de data/hora da última atualização na parte superior da página. Você também pode clicar no botão Download para baixar dados para uma pasta de trabalho do Excel. A operação

de download é executada em segundo plano e apresenta as informações mais recentes relatadas para o volume selecionado. Se a digitalização voltar sem resultados, certifique-se de que o volume está online. Eventos como o SnapRestore farão com que a análise do sistema de arquivos reconstrua sua lista de grandes diretórios.

Passos

1. Selecione **armazenamento > volumes**. Selecione o volume pretendido.
2. No menu volume individual, selecione **sistema de ficheiros**. Em seguida, selecione a guia **Usage**.
3. Alterne a opção **Analytics** para ativar a análise de uso.
4. O System Manager exibirá um gráfico de barras identificando os diretórios com o maior tamanho em ordem decrescente.

> O ONTAP pode exibir dados parciais ou nenhum dado enquanto a lista de diretórios superiores está sendo coletada. O progresso da digitalização pode estar no separador **Usage** (utilização) que é apresentado durante a digitalização.

Para obter mais informações sobre um diretório específico, você pode exibir atividade em um sistema de arquivos.

Tome medidas corretivas com base em análises

A partir do ONTAP 9.9,1, você pode tomar ações corretivas com base nos dados atuais e nos resultados desejados diretamente a partir das telas de análise do sistema de arquivos.

Excluir diretórios e arquivos

No visor do Explorer, pode selecionar diretórios ou ficheiros individuais para eliminar. Os diretórios são excluídos com a funcionalidade de exclusão assíncrona de diretório de baixa latência. (A exclusão assíncrona de diretório também está disponível a partir do ONTAP 9.9,1 sem a análise ativada.)

Passos

1. Clique em **Storage > volumes** e, em seguida, clique em **Explorer**.

   Quando você passa o Mouse sobre um arquivo ou pasta, a opção para excluir é exibida. Você só pode excluir um objeto de cada vez.

> Quando diretórios e arquivos são excluídos, os novos valores de capacidade de armazenamento não são exibidos imediatamente.

Atribua custo de Mídia em camadas de storage para comparar custos de locais de storage de dados inativos

O custo de Mídia é um valor que você atribui com base em sua avaliação dos custos de armazenamento, representado como sua moeda escolhida por GB. Quando definido, o System Manager usa o custo de Mídia atribuído para projetar economias estimadas ao mover volumes.

O custo de Mídia definido não é persistente; ele só pode ser definido para uma única sessão do navegador.

Passos

1. Clique em **armazenamento > camadas** e, em seguida, clique em **Definir custo de Mídia** nos blocos de nível local desejado (agregado).

   Certifique-se de selecionar níveis ativos e inativos para permitir a comparação.

2. Introduza um tipo de moeda e um montante.

   Quando introduz ou altera o custo do material, a alteração é efetuada em todos os tipos de material.

Mova volumes para reduzir custos de storage

Com base em exibições de análise e comparações de custo de Mídia, você pode migrar volumes para um storage mais barato em camadas locais.

Apenas um volume de cada vez pode ser comparado e movido.

Passos

1. Depois de ativar a exibição de custo de Mídia, clique em **armazenamento > camadas** e, em seguida, clique em **volumes**.
2. Para comparar as opções de destino de um volume, clique ⋮ em para o volume e, em seguida, clique em **mover**.
3. No visor **Select Destination local Tier** (Selecionar nível local de destino), selecione Destination Tiers (níveis de destino) para apresentar a diferença de custo estimada.
4. Depois de comparar as opções, selecione o nível desejado e clique em **mover**.

Controles de acesso baseados em função com File System Analytics

A partir do ONTAP 9.12,1, o ONTAP inclui uma função pré-definida de controle de acesso baseado em função (RBAC) `admin-no-fsa` chamada . A `admin-no-fsa` função concede Privileges de nível de administrador, mas impede que o usuário execute operações relacionadas ao `files` endpoint (ou seja, análise do sistema de arquivos) na CLI do ONTAP, API REST e no Gerenciador de sistema.

Para obter mais informações sobre a `admin-no-fsa` função, Funções predefinidas para administradores de clusterconsulte .

Se você estiver usando uma versão do ONTAP lançada antes do ONTAP 9.12,1, será necessário criar uma função dedicada para controlar o acesso à análise do sistema de arquivos. Nas versões do ONTAP anteriores ao ONTAP 9.12,1, é necessário configurar permissões RBAC por meio da CLI do ONTAP ou da API REST do ONTAP.

System Manager

A partir do ONTAP 9.12,1, você pode configurar permissões RBAC para análise do sistema de arquivos usando o Gerenciador de sistema.

Passos

1. Selecione **Cluster > Settings**. Em **Segurança**, navegue até **usuários e funções** e →selecione .
2. Em **funções**, + Add selecione .
3. Forneça um nome para a função. Em atributos de função, configure o acesso ou as restrições para a função de usuário fornecendo o "Pontos de extremidade API"apropriado . Consulte a tabela abaixo para ver os caminhos primários e os caminhos secundários para configurar as restrições ou o acesso ao File System Analytics.

Restrição	Caminho primário	Caminho secundário
Monitorização de atividade em volumes	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Monitorização de atividades em SVMs	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Todas as operações de análise do sistema de arquivos	`/api/storage/volumes`	`/:uuid/files`

   Você pode usar `/*/` em vez de um UUID para definir a política para todos os volumes ou SVMs no endpoint.

   Escolha o Access Privileges para cada endpoint.

4. Selecione **Guardar**.
5. Para atribuir a função a um utilizador ou utilizadores, Controle o acesso do administradorconsulte .

CLI

Se você estiver usando uma versão do ONTAP lançada antes do ONTAP 9.12,1, use a CLI do ONTAP para criar uma função personalizada.

Passos

1. Crie uma função padrão para ter acesso a todos os recursos.

   Isso precisa ser feito antes de criar a função restritiva para garantir que a função seja apenas restritiva no acompanhamento de atividades:

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. Crie a função restritiva:

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. Autorize funções para acessar os serviços da Web do SVM:

   - `rest` Para chamadas de API REST
   - `security` para proteção por senha
   - `sysmgr` Para acesso ao System Manager

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin

     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver svm-name -name sysmgr -role
   storageAdmin
   ```

4. Crie um usuário.

   Você deve emitir um comando criar distinto para cada aplicativo que deseja aplicar ao usuário. Chamadas criar várias vezes no mesmo usuário simplesmente aplica todos os aplicativos a esse usuário e não cria um novo usuário a cada vez. O `http` parâmetro para o tipo de aplicativo se aplica à API REST do ONTAP e ao Gerenciador de sistema.

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. Com as novas credenciais de usuário, agora você pode fazer login no Gerenciador de sistemas ou usar a API REST do ONTAP para acessar os dados de análise de sistemas de arquivos.

Mais informações

- Funções predefinidas para administradores de cluster
- Controle o acesso do administrador com o System Manager
- "Saiba mais sobre as funções RBAC e a API REST do ONTAP"

Considerações para análise do sistema de arquivos

Você deve estar ciente de certos limites de uso e possíveis impactos no desempenho

associados à implementação do File System Analytics.

Relacionamentos protegidos por SVM

Se você tiver habilitado a análise do sistema de arquivos em volumes com SVM em um relacionamento de proteção, os dados de análise não serão replicados para o SVM de destino. Se o SVM de origem precisar ser ressincronizado em uma operação de recuperação, será necessário rehabilitar manualmente as análises dos volumes desejados após a recuperação.

Considerações de desempenho

Em alguns casos, a ativação do File System Analytics pode afetar negativamente o desempenho durante a coleta inicial de metadados. Isso geralmente é visto em sistemas que estão na utilização máxima. Para evitar a ativação de análises em tais sistemas, você pode usar as ferramentas de monitoramento de desempenho do Gerenciador do sistema do ONTAP.

Se você tiver um aumento notável na latência, consulte o artigo da base de dados de Conhecimento "Latência alta ou flutuante após ativar a análise do sistema de arquivos do NetApp ONTAP".

Considerações de digitalização

Quando você ativa o análise de capacidade, o ONTAP realiza uma verificação de inicialização para análise de capacidade. A verificação acessa metadados para todos os arquivos em volumes para os quais a análise de capacidade está ativada. Nenhum dado de ficheiro é lido durante a digitalização. A partir do ONTAP 9.14,1, você pode acompanhar o andamento da verificação com a API REST, na guia **Explorer** do Gerenciador de sistema ou com o `volume analytics show` comando CLI. Se houver um evento de limitação, o ONTAP fornecerá uma notificação.

Ao ativar a análise do sistema de arquivos em um volume, certifique-se de que pelo menos 5 a 8% do espaço disponível do volume esteja livre. Se o volume tiver o dimensionamento automático ativado, calcule o tamanho disponível com base no tamanho máximo do crescimento automático. A partir do ONTAP 9.15,1, o ONTAP apresenta uma mensagem de erro se não houver espaço suficiente disponível quando você ativar a análise do sistema de arquivos em um volume.

Após a conclusão da verificação, o File System Analytics é atualizado continuamente em tempo real à medida que o sistema de arquivos muda.

O tempo necessário para a digitalização é proporcional ao número de diretórios e ficheiros no volume. Como a digitalização coleta metadados, o tamanho do arquivo não afeta o tempo de digitalização.

Para obter mais informações sobre a digitalização de inicialização, "TR-4867: Diretrizes de melhores práticas para análise de sistemas de arquivos"consulte .

Práticas recomendadas

Você deve iniciar a verificação em volumes que não compartilham agregados. Você pode ver quais agregados estão hospedando atualmente quais volumes usando o comando:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Enquanto a verificação é executada, os volumes continuam a servir o tráfego do cliente. Recomenda-se que inicie a verificação durante períodos em que antecipe um menor tráfego de clientes.

Se o tráfego do cliente aumentar, ele irá consumir recursos do sistema e fazer com que a varredura leve mais tempo.

A partir do ONTAP 9.12,1, você pode pausar a coleta de dados no Gerenciador do sistema e com a CLI do ONTAP.

- Se você estiver usando a CLI do ONTAP:
  - Você pode pausar a coleta de dados com o comando: `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - Uma vez que o tráfego do cliente abrandou, você pode retomar a coleta de dados com o comando: `volume analytics initialization resume -vserver svm_name -volume volume_name`
- Se você estiver usando o System Manager, na exibição **Explorer** do menu de volume, use os botões **Pausa coleta de dados** e **Resume coleta de dados** para gerenciar a digitalização.

Configuração EMS

Visão geral da configuração EMS

Você pode configurar o ONTAP 9 para enviar notificações de eventos importantes do EMS (sistema de gerenciamento de eventos) diretamente para um endereço de e-mail, servidor syslog, traphost de protocolo de rede de gerenciamento simples (SNMP) ou aplicativo webhook para que você seja imediatamente notificado sobre problemas do sistema que exigem atenção imediata.

Como as notificações de eventos importantes não estão habilitadas por padrão, você precisa configurar o EMS para enviar notificações para um endereço de e-mail, um servidor syslog, um traphost SNMP ou um aplicativo webhook.

Reveja as versões específicas da versão do "Referência EMS da ONTAP 9".

Se o mapeamento de eventos do EMS usar conjuntos de comandos ONTAP obsoletos (como destino de eventos, rota de eventos), é recomendável atualizar o mapeamento. "Saiba como atualizar seu mapeamento EMS a partir de comandos ONTAP obsoletos".

Configurar notificações e filtros de eventos EMS com o System Manager

Você pode usar o System Manager para configurar como o sistema de gerenciamento de eventos (EMS) entrega notificações de eventos para que você possa ser notificado sobre problemas do sistema que exigem sua atenção imediata.

Versão de ONTAP	Com o System Manager, você pode…
ONTAP 9.12,1 e posterior	Especifique o protocolo TLS (Transport Layer Security) ao enviar eventos para servidores syslog remotos.
ONTAP 9.10,1 e posterior	Configure endereços de e-mail, servidores syslog e aplicativos de webhook, bem como hosts SNMP.
ONTAP 9 F.7 a 9.10.0	Configurar apenas os hosts SNMP. Você pode configurar outro destino EMS com a CLI do ONTAP. "Visão geral da configuração EMS"Consulte .

Você pode executar os seguintes procedimentos:

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

Informações relacionadas

- "Referência EMS da ONTAP"
- "Usando a CLI para configurar hosts SNMP para receber notificações de eventos"

Adicionar um destino de notificação de evento EMS

Você pode usar o System Manager para especificar para onde deseja que as mensagens EMS sejam enviadas.

A partir do ONTAP 9.12,1, os eventos EMS podem ser enviados para uma porta designada em um servidor syslog remoto através do protocolo TLS (Transport Layer Security). Para obter detalhes, consulte a `event notification destination create` página de manual.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Clique em + Add .
5. Especifique um nome, um tipo de destino EMS e filtros.

   Se necessário, você pode adicionar um novo filtro. Clique em **Adicionar um novo filtro de evento**.

6. Dependendo do tipo de destino EMS selecionado, especifique o seguinte:

Para configurar…	Especificar ou selecionar…
SNMP traphost	• Nome do Traphost
E-mail (Começando com 9.10.1)	• Endereço de e-mail de destino • Servidor de correio • Do endereço de e-mail

Servidor syslog (Começando com 9.10.1)	• Nome do host ou endereço IP do servidor • Porta syslog (começando com 9.12.1) • Transporte syslog (começando com 9.12.1) Selecionar **TCP Encrypted** ativa o protocolo TLS (Transport Layer Security). Se nenhum valor for inserido para **Syslog port**, um padrão será usado com base na seleção **Syslog transport**.
Webhook (Começando com 9.10.1)	• URL do webhook • Autenticação de cliente (selecione esta opção para especificar um certificado de cliente)

Crie um novo filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para definir novos filtros personalizados que especificam as regras para o tratamento de notificações EMS.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Clique Add em .
5. Especifique um nome e selecione se deseja copiar regras de um filtro de evento existente ou adicionar novas regras.
6. Dependendo da sua escolha, execute as seguintes etapas:

Se você escolher…	Em seguida, execute estes passos…
Copiar regras do filtro de eventos existente	1. Selecione um filtro de eventos existente. 2. Modifique as regras existentes. 3. Adicione outras regras, se necessário, clicando Add em .
Adicione novas regras	Especifique o tipo, o padrão de nome, as severidades e o tipo de trap SNMP para cada nova regra.

Editar um destino de notificação de evento EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para alterar as informações de destino da notificação de eventos.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.

4. Ao lado do nome do destino do evento, clique em e, em seguida, clique em **Editar**.
5. Modifique as informações de destino do evento e clique em **Salvar**.

Editar um filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para modificar filtros personalizados para alterar a forma como as notificações de eventos são tratadas.

Não é possível modificar filtros definidos pelo sistema.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Ao lado do nome do filtro de evento, clique em e, em seguida, clique em **Editar**.
5. Modifique as informações do filtro de eventos e clique em **Salvar**.

Eliminar um destino de notificação de evento EMS

A partir do ONTAP 9.10,1, pode utilizar o Gestor do sistema para eliminar um destino de notificação de eventos EMS.

Não é possível eliminar destinos SNMP.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Ao lado do nome do destino do evento, clique em e, em seguida, clique em **Excluir**.

Eliminar um filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para excluir filtros personalizados.

Não é possível eliminar filtros definidos pelo sistema.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Ao lado do nome do filtro de evento, clique em e, em seguida, clique em **Eliminar**.

Configure as notificações de eventos EMS com a CLI

Fluxo de trabalho de configuração do EMS

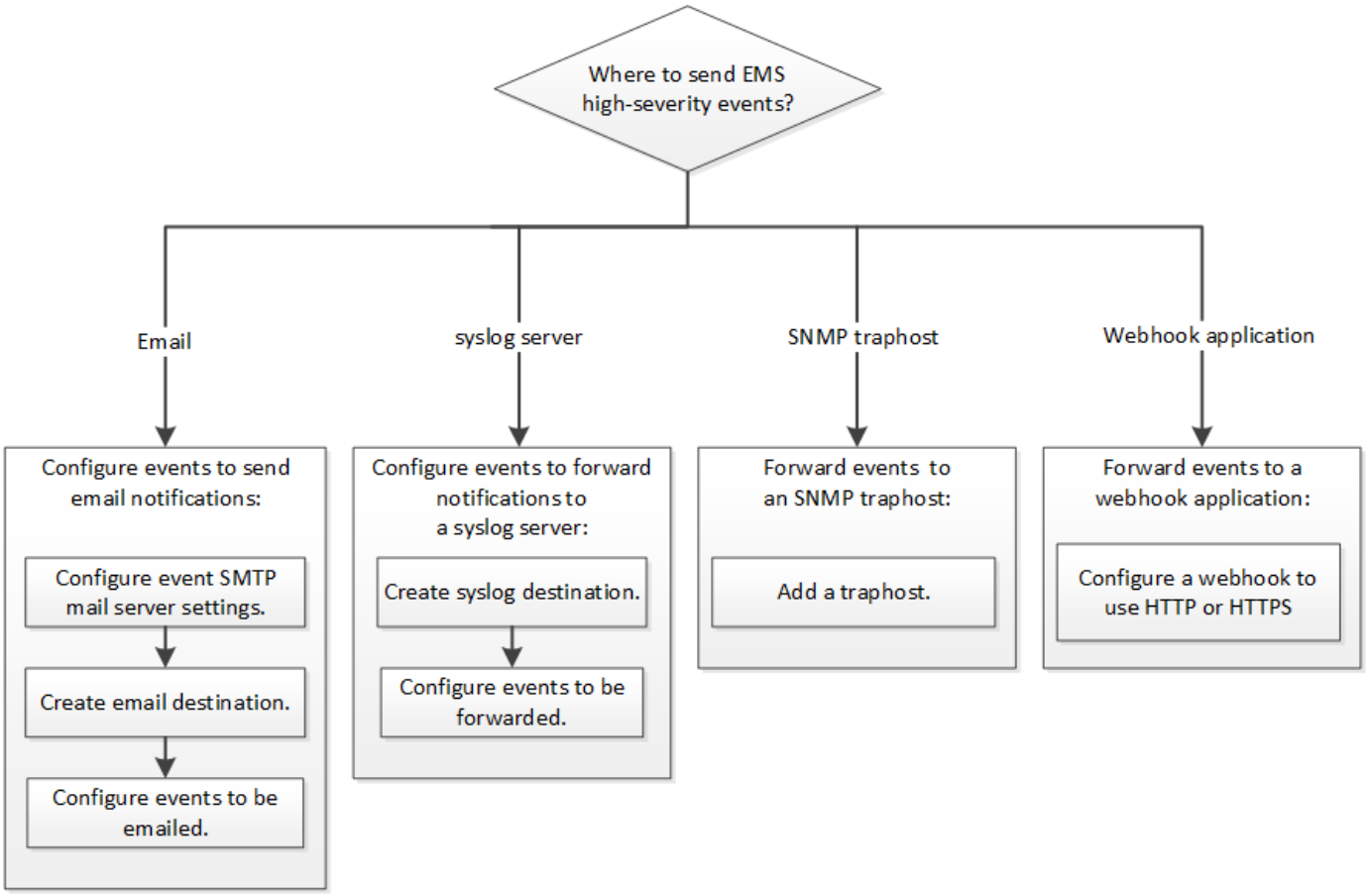
Você deve configurar notificações importantes de eventos EMS para serem enviadas como e-mail, encaminhadas para um servidor syslog, encaminhadas para um traphost SNMP ou encaminhadas para um aplicativo webhook. Isso ajuda você a evitar interrupções no sistema, tomando ações corretivas em tempo hábil.

Sobre esta tarefa

Se o seu ambiente já contém um servidor syslog para agregar os eventos registrados de outros sistemas, como servidores e aplicativos, então é mais fácil usar esse servidor syslog também para notificações de eventos importantes de sistemas de armazenamento.

Se o seu ambiente ainda não contém um servidor syslog, é mais fácil usar e-mail para notificações de eventos importantes.

Se você já encaminhar notificações de eventos para um traphost SNMP, talvez queira monitorar esse traphost para eventos importantes.



Opções

- Defina EMS para enviar notificações de eventos.

Se você quiser…	Consulte isto…
O EMS para enviar notificações de eventos importantes para um endereço de e-mail	Configurar eventos importantes do EMS para enviar notificações por e-mail

O EMS para encaminhar notificações de eventos importantes para um servidor syslog	Configure eventos importantes do EMS para encaminhar notificações para um servidor syslog
Se você quiser que o EMS encaminhe notificações de eventos para um traphost SNMP	Configure os hosts SNMP para receber notificações de eventos
Se você quiser que o EMS encaminhe notificações de eventos para um aplicativo webhook	Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook

Configurar eventos importantes do EMS para enviar notificações por e-mail

Para receber notificações por e-mail dos eventos mais importantes, você deve configurar o EMS para enviar mensagens de e-mail para eventos que sinalizem atividade importante.

O que você vai precisar

O DNS deve ser configurado no cluster para resolver os endereços de e-mail.

Sobre esta tarefa

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na linha de comando ONTAP.

Passos

1. Configure as definições do servidor de correio SMTP de eventos:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. Criar um destino de e-mail para notificações de eventos:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. Configure os eventos importantes para enviar notificações por e-mail:

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

Configurando eventos importantes do EMS para encaminhar notificações para um servidor syslog

Para Registrar notificações dos eventos mais graves em um servidor syslog, você deve configurar o EMS para encaminhar notificações de eventos que sinalizam atividade importante.

O que você vai precisar

O DNS deve ser configurado no cluster para resolver o nome do servidor syslog.

Sobre esta tarefa

Se o seu ambiente ainda não contiver um servidor syslog para notificações de eventos, você deve primeiro criar um. Se o seu ambiente já contiver um servidor syslog para registar eventos de outros sistemas, talvez você queira usá-lo para notificações de eventos importantes.

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na CLI do ONTAP.

A partir do ONTAP 9.12,1, os eventos EMS podem ser enviados para uma porta designada em um servidor syslog remoto através do protocolo TLS (Transport Layer Security). Dois novos parâmetros estão disponíveis:

`tcp-encrypted`

Quando `tcp-encrypted` for especificado para o `syslog-transport`, o ONTAP verifica a identidade do host de destino validando seu certificado. O valor padrão é `udp-unencrypted`.

`syslog-port`

O parâmetro valor padrão `syslog-port` depende da configuração do `syslog-transport` parâmetro. Se `syslog-transport` estiver definido como `tcp-encrypted`, `syslog-port` tem o valor padrão 6514.

Para obter detalhes, consulte a `event notification destination create` página de manual.

Passos

1. Crie um destino de servidor syslog para eventos importantes:

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   A partir de ONTAP 9.12,1, os seguintes valores podem ser especificados para `syslog-transport`:

   - `udp-unencrypted` - Protocolo de datagrama de usuário sem segurança
   - `tcp-unencrypted` - Protocolo de Controle de transmissão sem segurança
   - `tcp-encrypted` - Protocolo de Controle de transmissão com Transport Layer Security (TLS)

   O protocolo predefinido é `udp-unencrypted`.

2. Configure os eventos importantes para encaminhar notificações para o servidor syslog:

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

Configure os hosts SNMP para receber notificações de eventos

Para receber notificações de eventos em um traphost SNMP, você deve configurar um traphost.

O que você vai precisar

- Os traps SNMP e SNMP devem estar ativados no cluster.

  As traps SNMP e SNMP estão ativadas por predefinição.

- O DNS deve ser configurado no cluster para resolver os nomes do traphost.

Sobre esta tarefa

Se você ainda não tiver um traphost SNMP configurado para receber notificações de eventos (traps SNMP), você deve adicionar um.

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na linha de comando ONTAP.

Passo

1. Se o seu ambiente ainda não tiver um traphost SNMP configurado para receber notificações de eventos, adicione uma:

   `system snmp traphost add -peer-address` *`snmp_traphost_name`*

   Todas as notificações de eventos que são suportadas por SNMP por padrão são encaminhadas para o traphost SNMP.

Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook

Você pode configurar o ONTAP para encaminhar notificações de eventos importantes para um aplicativo webhook. As etapas de configuração necessárias dependem do nível de segurança escolhido.

Prepare-se para configurar o encaminhamento de eventos EMS

Há vários conceitos e requisitos que você deve considerar antes de configurar o ONTAP para encaminhar notificações de eventos para um aplicativo webhook.

Aplicação webhook

Você precisa de um aplicativo webhook capaz de receber as notificações de eventos do ONTAP. Um webhook é uma rotina de retorno de chamada definida pelo usuário que estende a capacidade do aplicativo ou servidor remoto onde ele é executado. Webhooks são chamados ou ativados pelo cliente (neste caso ONTAP) enviando uma solicitação HTTP para o URL de destino. Especificamente, o ONTAP envia uma solicitação HTTP POST para o servidor que hospeda o aplicativo webhook junto com os detalhes de notificação de evento formatados em XML.

Opções de segurança

Existem várias opções de segurança disponíveis, dependendo de como o protocolo TLS (Transport Layer Security) é usado. A opção escolhida determina a configuração necessária do ONTAP.

> TLS é um protocolo criptográfico amplamente utilizado na internet. Ele fornece privacidade, bem como integridade de dados e autenticação usando um ou mais certificados de chave pública. Os certificados são emitidos por autoridades de certificação confiáveis.

HTTP

Você pode usar HTTP para transportar as notificações de eventos. Com esta configuração, a conexão não é segura. As identidades do cliente ONTAP e da aplicação webhook não são verificadas. Além disso, o tráfego de rede não é criptografado ou protegido. "Configure um destino de webhook para usar HTTP"Consulte para obter os detalhes de configuração.

HTTPS

Para segurança adicional, você pode instalar um certificado no servidor que hospeda a rotina do webhook. O protocolo HTTPS é usado pelo ONTAP para verificar a identidade do servidor de aplicativos webhook, bem como por ambas as partes para garantir a privacidade e integridade do tráfego de rede. "Configure um destino de webhook para usar HTTPS"Consulte para obter os detalhes de configuração.

HTTPS com autenticação mútua

Você pode aprimorar ainda mais a segurança HTTPS instalando um certificado de cliente no sistema ONTAP que emite as solicitações de webbook. Além de o ONTAP verificar a identidade do servidor de aplicativos webhook e proteger o tráfego de rede, o aplicativo webhook verifica a identidade do cliente ONTAP. Essa autenticação de dois sentidos é conhecida como *Mutual TLS*. "Configure um destino de webhook para usar HTTPS com autenticação mútua"Consulte para obter os detalhes de configuração.

Informações relacionadas

- "O protocolo TLS (Transport Layer Security) versão 1,3"

Configure um destino de webhook para usar HTTP

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo webhook usando HTTP. Esta é a opção menos segura, mas a mais simples de configurar.

Passos

1. Crie um novo destino `restapi-ems` para receber os eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   No comando acima, você deve usar o esquema **HTTP** para o destino.

2. Crie uma notificação vinculando o `important-events` filtro ao `restapi-ems` destino:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configure um destino de webhook para usar HTTPS

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo de webhook usando HTTPS. O ONTAP usa o certificado do servidor para confirmar a identidade do aplicativo webhook, bem como proteger o tráfego de rede.

Antes de começar

- Gerar uma chave privada e um certificado para o servidor de aplicativos webhook
- Tenha o certificado raiz disponível para instalação no ONTAP

Passos

1. Instale a chave privada do servidor e os certificados apropriados no servidor que hospeda seu aplicativo webhook. As etapas de configuração específicas dependem do servidor.
2. Instale o certificado raiz do servidor no ONTAP:

   ```
   security certificate install -type server-ca
   ```

   O comando pedirá o certificado.

3. Crie o `restapi-ems` destino para receber os eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   No comando acima, você deve usar o esquema **HTTPS** para o destino.

4. Crie a notificação que vincula o `important-events` filtro ao novo `restapi-ems` destino:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configure um destino de webhook para usar HTTPS com autenticação mútua

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo de webhook usando HTTPS com autenticação mútua. Com esta configuração existem dois certificados. O ONTAP usa o certificado do servidor para confirmar a identidade do aplicativo webhook e proteger o tráfego de rede. Além disso, o aplicativo que hospeda o webhook usa o certificado de cliente para confirmar a identidade do cliente ONTAP.

Antes de começar

Você deve fazer o seguinte antes de configurar o ONTAP:

- Gerar uma chave privada e um certificado para o servidor de aplicativos webhook
- Tenha o certificado raiz disponível para instalação no ONTAP
- Gerar uma chave privada e um certificado para o cliente ONTAP

Passos

1. Execute as duas primeiras etapas da tarefa "Configure um destino de webhook para usar HTTPS" para instalar o certificado do servidor para que o ONTAP possa verificar a identidade do servidor.
2. Instale os certificados raiz e intermediários apropriados no aplicativo webhook para validar o certificado do cliente.
3. Instale o certificado de cliente no ONTAP:

   ```
   security certificate install -type client
   ```

   O comando pedirá a chave privada e o certificado.

4. Crie o `restapi-ems` destino para receber os eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   No comando acima, você deve usar o esquema **HTTPS** para destino.

5. Crie a notificação que vincula o `important-events` filtro ao novo `restapi-ems` destino:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Atualizar mapeamento de eventos EMS obsoleto

Modelos de mapeamento de eventos EMS

Antes do ONTAP 9.0, os eventos EMS só podiam ser mapeados para destinos de eventos com base na correspondência do padrão de nomes de eventos. Os conjuntos de comandos ONTAP (`event destination`, `event route`) que utilizam este modelo continuam a estar disponíveis nas versões mais recentes do ONTAP, mas foram obsoletos a partir do ONTAP 9.0.

A partir do ONTAP 9.0, a melhor prática para o mapeamento de destino de eventos do ONTAP EMS é usar o modelo de filtro de eventos mais dimensionável no qual a correspondência de padrões é feita em vários campos, usando os `event filter` conjuntos de comandos , `event notification` e `event notification destination` .

Se o mapeamento EMS estiver configurado usando os comandos obsoletos, você deverá atualizar o mapeamento para usar os `event filter` conjuntos de comandos , `event notification` e `event notification destination` .

Existem dois tipos de destinos de eventos:

1. **Destinos gerados pelo sistema**: Existem cinco destinos de eventos gerados pelo sistema (criados por padrão)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     Alguns dos destinos gerados pelo sistema são para fins especiais. Por exemplo, o destino asup encaminha os eventos callhome.* para o módulo AutoSupport no ONTAP para gerar mensagens AutoSupport.
2. **Destinos criados pelo usuário**: Estes são criados manualmente usando o `event destination create` comando.

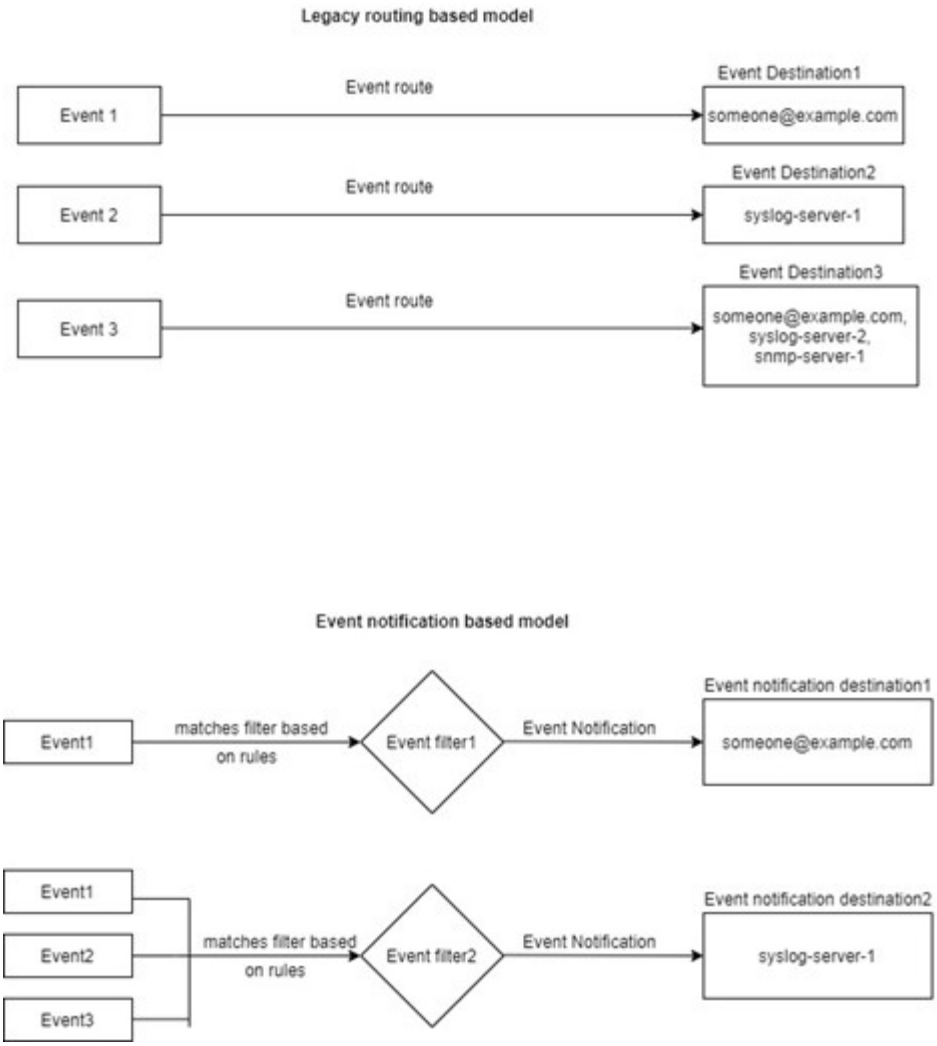
```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

No modelo obsoleto, os eventos EMS são mapeados individualmente para um destino usando o `event route add-destinations` comando.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

O novo e mais escalável mecanismo de notificações de eventos EMS baseia-se em filtros de eventos e destinos de notificação de eventos. Consulte o seguinte artigo da KB para obter informações detalhadas sobre o novo mecanismo de notificação de eventos:

- "Visão geral do sistema de gerenciamento de eventos para ONTAP 9"



Atualize o mapeamento de eventos do EMS a partir de comandos ONTAP obsoletos

Se o mapeamento de eventos do EMS estiver configurado atualmente usando os conjuntos de comandos ONTAP obsoletos (`event destination`, `event route`), siga este procedimento para atualizar o mapeamento para usar os `event filter` conjuntos de comandos , `event notification` e `event notification destination` .

Passos

1. Liste todos os destinos de eventos no sistema usando o `event destination show` comando.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. Para cada destino, liste os eventos que estão sendo mapeados usando o `event route show -destinations <destination name>` comando.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

3. Crie um correspondente `event filter` que inclua todos esses subconjuntos de eventos. Por exemplo, se você quiser incluir apenas os `raid.aggr.`eventos *, use um caractere curinga para o `message-name` parâmetro ao criar o filtro. Você também pode criar filtros para eventos individuais.

Você pode criar até 50 filtros de eventos.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Criar um `event notification destination` para cada um `event destination` dos endpoints (ou seja, SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. Crie uma notificação de evento mapeando o filtro de evento para o destino de notificação de evento.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------ -----------------
1    default-trap-events            snmp-traphost
2    asup_events                    dest1
2 entries were displayed.
```

6. Repita as etapas 1-5 para cada `event destination` um que tenha um `event route` mapeamento.

Os eventos roteados para destinos SNMP devem ser mapeados para o `snmp-traphost` destino de notificação de eventos. O destino SNMP traphost usa o sistema SNMP traphost configurado.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

               Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

Referência do comando ONTAP

Para cada versão principal do ONTAP, os comandos CLI comumente disponíveis (páginas manuais do ONTAP ou páginas man) são agrupados em uma *referência de comando*. Essas referências de comando explicam como usar os comandos CLI em cada versão do ONTAP. Páginas man também estão disponíveis na linha de comando ONTAP com o `man` comando. Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Referências de comandos para versões suportadas do ONTAP

- "ONTAP 9.16,1"
- "ONTAP 9.15,1"
- "ONTAP 9.14,1"
- "ONTAP 9.13,1"
- "ONTAP 9.12,1"
- "ONTAP 9.11,1"
- "ONTAP 9.10,1"
- "ONTAP 9.9,1"
- "ONTAP 9,8"
- "ONTAP 9,7"
- "ONTAP 9,6"
- "ONTAP 9,5"
- "ONTAP 9,3"

Referências de comandos para versões de suporte limitado do ONTAP (apenas PDF)

- "ONTAP 9,4"
- "ONTAP 9,2"
- "ONTAP 9,1"

Ferramenta de comparação CLI

Você pode aprender sobre alterações nos comandos da interface de linha de comando (CLI) entre as versões do ONTAP usando o "Ferramenta de comparação CLI" no site de suporte da NetApp.

Leitura adicional

- Use a interface de linha de comando ONTAP
- Métodos de navegação de diretórios de comando CLI

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

ONTAP

"Aviso para ONTAP 9.16,1" "Aviso para ONTAP 9.16,0" "Aviso para ONTAP 9.15,1" "Aviso para ONTAP 9.15,0" "Aviso para ONTAP 9.14,1" "Aviso para ONTAP 9.14,0" "Aviso para ONTAP 9.13,1" "Aviso para ONTAP 9.12,1" "Aviso para ONTAP 9.12,0" "Aviso para ONTAP 9.11,1" "Aviso para ONTAP 9.10,1" "Aviso para ONTAP 9.10,0" "Aviso para ONTAP 9.9,1" "Aviso para ONTAP 9.8" "Aviso para ONTAP 9.7" "Aviso para ONTAP 9.6" "Aviso para ONTAP 9.5" "Aviso para ONTAP 9.4" "Aviso para ONTAP 9.3" "Aviso para ONTAP 9.2" "Aviso para ONTAP 9.1"

ONTAP Mediador para configurações MetroCluster IP

"9.9.1 Aviso para o Mediador ONTAP para configurações MetroCluster IP" "9,8 Aviso para o Mediador ONTAP para configurações MetroCluster IP" "9,7 Aviso para o Mediador ONTAP para configurações MetroCluster IP"

Informações sobre direitos autorais

Informações sobre marcas comerciais